State of Alaska
Election Security Project:
Election Process Review
Phase 3 Report

June 29, 2012 Final Review Draft - Revision 28

Prepared for State of Alaska Division of Elections

UNIVERSITY *of* ALASKA ANCHORAGE

Table of Contents

Study Team

The analysis was conducted by a cross-organizational team from University of Alaska Anchorage and industry.

Principal Investigator

LuAnn Piccard, PMP, Assistant Professor and Interim Director of the Engineering, Science, and Project Management Programs, School of Engineering. She was Principal Investigator for Phase 1 and 2 of the State of Alaska Election Security Projects.

Research Team

Roger Hull, CISSP, CSM, CRISC, PMP, Instructor for the Project Management Department, School of Engineering.

Mark Ayers, P.E., Consultant and Adjunct Faculty Member, School of Engineering.

Dr. David B. Hoffman, Adjunct Professor for the Engineering and Science Management and Project Management graduate programs, School of Engineering. He is a retired professor from University of Alaska Fairbanks and a consultant in process mapping/modeling, simulation and decision support techniques.

Dr. Stephanie Martin, Assistant Professor of Economics and Public Policy, Institute of Social and Economic Research (ISER). Dr. Martin has worked on the Election Security and Election Translation projects. She has also conducted research on criminal justice, migration, well-being of indigenous people, and several evaluation studies.

Mary Killorin, Research Associate, Institute of Social and Economic Research (ISER).

Patricia Deroche, Research Associate, Institute of Social and Economic Research (ISER).

Michelle L. Webb, Project Coordinator and Engineering, Science and Project Management Program staff member. She is currently pursuing master's studies in both Public Administration and Project Management.

Acknowledgements

The study team gratefully acknowledges help from many people in the preparation of this report.

Alaska Lieutenant Governor Mead Treadwell

Michelle Toohey, Alaska Lieutenant Governor Mead Treadwell's Chief of Staff

Alaska Division of Elections

- Gail Fenumiai, State Director
- Shelly Growden, Election Systems Manager
- Julie Husmann, Region II Elections Supervisor (Districts 13-32: Municipality of Anchorage, Matanuska-Susitna Borough, Whittier and Hope Areas.

Real-time Voter History Solutions

Vendors

- Election Administrators (Martin White)
- Hart Intercivic (Jim Suver)

Jurisdictions Using RTVH Solutions

- Dianna J. Duran, the Secretary of State for New Mexico
- Dr. Brenda Snipes, Supervisor of Elections in Broward County, Florida
- The Staff and Officials of the Meklenberg County Board of Elections, North Carolina

RTVH Technical Advisors

- John Falconer, Applied Microsystems
- Ross Johnston, Owner, Finepoint Advertising
- Aaron Morse, Managing Member, Catapult Consulting
- Lance Ahern, CIO, Municipality of Anchorage
- Lauchie Johnston, LMJ Consulting

Executive Summary

In April 2011, the State of Alaska Office of Lieutenant Governor Mead Treadwell produced a 2010 General Election Review (Appendix B: 2010 General Election Review, April, 1, 2010). This report recommended a number of statutory and election procedure changes. In addition, several areas were recommended for third party review:

- Review of division's audit procedures and hand-count verification of election results.
- Audit to ensure non-U.S. citizens are not voting.
- Audit to ensure felons are not voting.
- Explore systems or methods that can provide for real-time voter history.

The above items were incremental to the scope of work conducted in the S*tate of Alaska Election Security Project (Phase 1 and 2, September 2007-May 2008)* (See Appendix C), conducted by the University of Alaska Anchorage. Additionally, the division asked for revalidation of two items that were included in that original project report:

- Revalidate election equipment security given recent certified, technology upgrades.
- Reassess end-to-end ballot security.

The Alaska Division of Elections requested that the University of Alaska Anchorage undertake the third party review to assess the above items. This study was completed during the period of June 2011-April 2012. This report builds upon the original State of Alaska Election Security Project (Phases 1 and 2). That study evaluated the overall security of Alaska's Election System including the integrity of the electronic voting systems, the procedures, processes and personnel of the election system overall, and the public's confidence in the outcomes of the election process. The report recommended a number of improvements to further strengthen the system. All of the recommendations made were accepted and implemented by the Division of Elections.

The goal of this third party review was to address a specific set of items identified in the 2010 General Election Review (See Appendix D: Division of Elections Election Process Review Scope of Work) including a review of tabulation equipment (new items implemented after 2008 study), ballot security (pre, during and post-election), and an audit of the post-election processes and procedures used by the Division of Elections in anticipation of the 2012 elections. This follow-on study was undertaken to identify those areas where improvements could be made to ensure the division's tabulation equipment, voter history, ballot security and review, and election audit procedures are secure, effective and maintain the public's trust in Alaska's election system. In addition, the division's processes to ensure non-U.S. citizens and felons convicted of moral turpitude are not registered and/or voting, were also reviewed. The team was also asked to evaluate potential solutions to provide real-time voter history on Election Day.

Scope of Work for Project

The specific items included in the scope of work for this project are described in detail in Appendix D: Division of Elections: Election Process Review Statement of Work, and include:

- Revalidate tabulation equipment security (items implemented based on 2008 report recommendations)
- Review ballot security (pre-, during and post-election)
- Review post-election audit procedures and hand-count verification procedures
- Review methods used by division relating to felons and non-U.S. citizens.
- Review systems that can improve real-time access to and more efficient processing of voter history (See Appendix E: Real-time Voter History Solution Evaluation)

In particular, the following items were evaluated:

Tabulation Equipment Security-Revalidate tabulation equipment security, building on a foundation of the original study completed in 2008.

Ballot Security - The processes used to secure ballots (pre-, during and post- election) during transit between various polling locations and the Division of Elections, as well as the security of the ballots once they are received by the division, will be reviewed to ensure ballots are secure and accounted for before, during and after transport, and to identify any necessary improvements. In addition, the processes and procedures relating to accountability and destruction of unvoted ballots after an election will be reviewed to ensure unvoted ballots cannot be later falsified and added to the election results. The study will identify improvements needed to ensure ballot accountability.

Post-election Audit Procedures – The methods and audit procedures used by the division's absentee and questioned ballot review boards and the State Ballot Counting Review Board (SRB), including the hand-count verification, to certify the election results should be reviewed to determine if the audit processes currently used would identify potential discrepancies in reported results and to recommend changes that would improve audit procedures. In addition, a review of the post-election processes would increase the public's confidence in the election results and identify any information that might be necessary to answer questions in the event of an election challenge.

Voter History – When entering a polling place, voters sign a precinct register before being given a ballot. The precinct boards return all registers to the Division of Elections office in their region, and division staff updates voter history on the official voter registration record. This history is entered manually by division staff and must be completed before the division opens and counts absentee and questioned ballots. In addition, in order for political parties and/or candidates to determine which voters have voted in an election, they currently need to station poll watchers at precincts to record voter names or wait until the division has performed the voter history. A review of the procedures used by the division to provide for voter history, researching the feasibility of implementing systems that might provide "real-time" access to and more efficient processing of voter history will be done to determine possible alternatives, including a cost/benefit analysis, timelines for, and risk assessment of such alternatives aligned with the 2012 election. (This review is included as Appendix E: Real-time Voter History Solution Evaluation)

Felons and Non-U.S. Citizens – The processes and procedures used by the division to ensure felons convicted of moral turpitude and non-U.S. Citizens are not registered and/or voting should be reviewed to determine if the division has access to, and receives information from, the necessary resources and data to identify such voters.

Out of Scope Items

Several items in the 2010 General Election Report (Appendix B) were handled through different forums and were not included in the scope of work for this report. In particular, poll worker training and mechanisms for Division of Elections to respond to and address public comment are not included. Please see Appendix B for further details.

This study also did not evaluate the implementation of electronic poll books (EPB) as an alternative to or replacement for paper registers in polling places and the resulting costs/benefits of such implementations. Research was restricted to the evaluation of EPB based Real-time Voter History (RTVH) solutions to determine the potential feasibility of implementing standalone RTVH capabilities within the context of the current polling place environment in Alaska. (See Appendix E: Real-time Voter History Solution Evaluation)

Significant Findings and Recommendations

The University of Alaska Anchorage research team has determined that the Alaska Election System remains secure. However, there are opportunities to fine tune the equipment and processes for even greater benefit. Some of these items were revealed as a result of the atypical senatorial write-in campaign during the 2010 general election. Another was identified based on a recent analysis of the Accu-Vote Touch Screen (AV-TSX) voting system conducted by Argonne National Laboratory Vulnerability Assessment Team and our independent validation of the issue. Others are more general recommendations given technology and workforce changes that will impact the longer term approach for the state's election system. This report recommends several additional election security measures and other general findings. The Division of Elections should:

- Add additional tamper evident seals on the AV-TSX (Touch Screen) voting system enclosure.
- Improve unused and spoiled ballot security at the precincts.
- Strengthen handling of voted ballots after receipt in Juneau and prior to hand-count verification.
- Continue efforts to strengthen integration of Alaska State Department of Corrections, U.S. Department of Homeland Security (Immigration), and other databases with the Voter Registration database.
- Utilize a comprehensive Election Auditability Checklist before, during and after each election (See Appendix F: Election Auditability Checklist)
- Implement a consistent and effective procedure to provide public record voter history information to interested parties on Election Day.
- Should not undertake implementation of a stand-alone, Real-time Voter History (RTVH) solution without further evaluation and within the context of a more comprehensive, long-range electronic voting strategy. (See as Appendix E: Real-time Voter History Solution Evaluation)
- Develop a mid-to-long range strategic plan for Alaska's Election System that includes the evaluation, adoption, and implementation of new technologies (including tabulation systems, databases, real-

time voter history solutions, electronic poll books, etc.) to support the changing needs of voters and election officials in Alaska and that address the associated and necessary evolution of procedures and workforce training to ensure a continuation of secure and participative elections.

Introduction

Alaska's Election System

Our findings indicate that Alaska's election system is among the most secure in the country, and it has a number of safeguards other states are now adopting. Given the state's huge size, limited road system, and scattered communities, Alaska has some unique challenges not faced by other states, to ensure the integrity of the vote.

Some of the key characteristics of Alaska's election system are:

- Centralized voting system with standard procedures and identical hardware and software throughout Alaska. This centralization minimizes opportunities for tampering and allows flaws identified in any part of the system to be corrected statewide.
- Paper back-ups for all votes. Although optical scanners do scan and count ballots in 305 of Alaska's 438 precincts, almost all voters mark paper ballots that serve as back-ups to electronic tallies. There are touch-screen machines in all precincts. However, only 1% of voters use those machines and they also have internal paper reels as back-ups. In Alaska, the paper ballot is considered the official vote.
- Independent verification and cross-checking of paper ballots, electronic tallies, and voter registration books.
- Audit of machine counts by votes using hand counts in a random sample of precincts in all 40 election districts in the state.
- Observers invited to watch both voting and vote-counting procedures.

Alaska measures its election security along the following dimensions:

Defense in Depth: A secure system should have multiple layers of protection so that if one fails, others are still in place. This layered approach can discourage intrusion because intruders would have to take several undetected steps to penetrate the system's security. Also, layers can provide early warning of attacks in time for election officials to take action. Equipment, people, and procedures together provide defense in depth.

Fortification of Systems: This means making electronic systems as secure as possible and using the latest certified updates, which may correct vulnerabilities identified in earlier systems. Alaska uses optical scanners that tally votes cast on paper ballots; touch-screen machines with internal paper reels that record the votes cast; and computer servers that integrate and tally the electronic and hand-count results. All of these systems should be equipped with the latest updates to minimize the potential for votes to be miscounted or tampered with, and they should be protected so unauthorized users can't

interfere with their operation before, during, or after elections. The systems must also be certified to federal standards and verified by independent testing centers.

Confidence in Outcomes: System and results must be verifiable and shown to be reliable in order to maintain both voters' and election officials' confidence in the system. The methods used to select a sample of results for hand-counting must also provide a high level of confidence. The election process must be open, so anyone can observe what is happening and verify that the election officials are objective and that partisan interests are balanced.

In Alaska, the lieutenant governor oversees the Division of Elections, and the Division of Elections manages federal and state elections statewide.

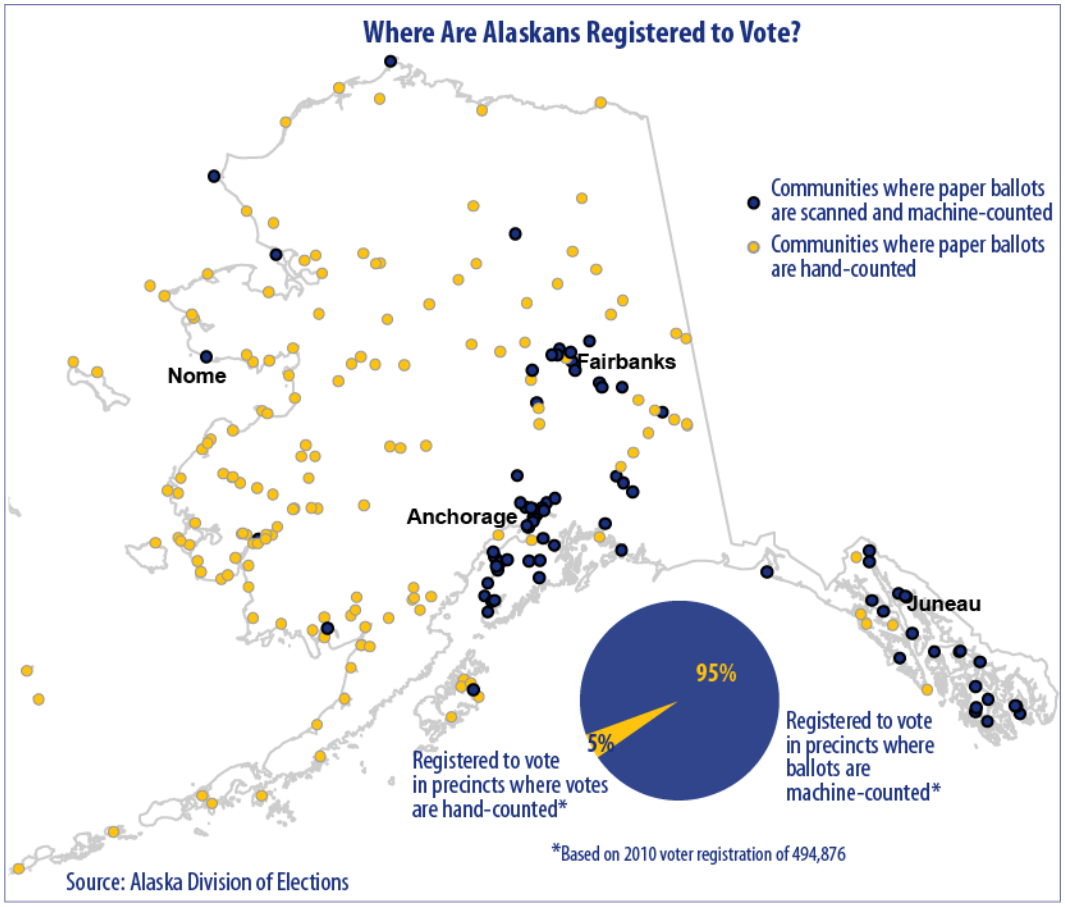
Alaska is divided into four election regions that include a total of 40 House Districts and 20 Senate Districts. Two House Districts combined make up a single Senate District. Each House District is further divided into precincts. There are 438 precincts in Alaska. There is one polling place for each precinct. In order to conduct an election, the Division of Elections must make sure that each precinct has a polling location, election workers to run the polling place, and that each location has the ballots, supplies, and equipment needed for the election.

For administrative purposes, the Division of Elections has four regional offices (previous to 2012 redistricting):

- Region I in Juneau includes Districts 1-5 and 33-36.
- Region II in Anchorage includes Districts 13-32.
- Region III in Fairbanks includes Districts 6-12.
- Region IV in Nome includes Districts 37-40.

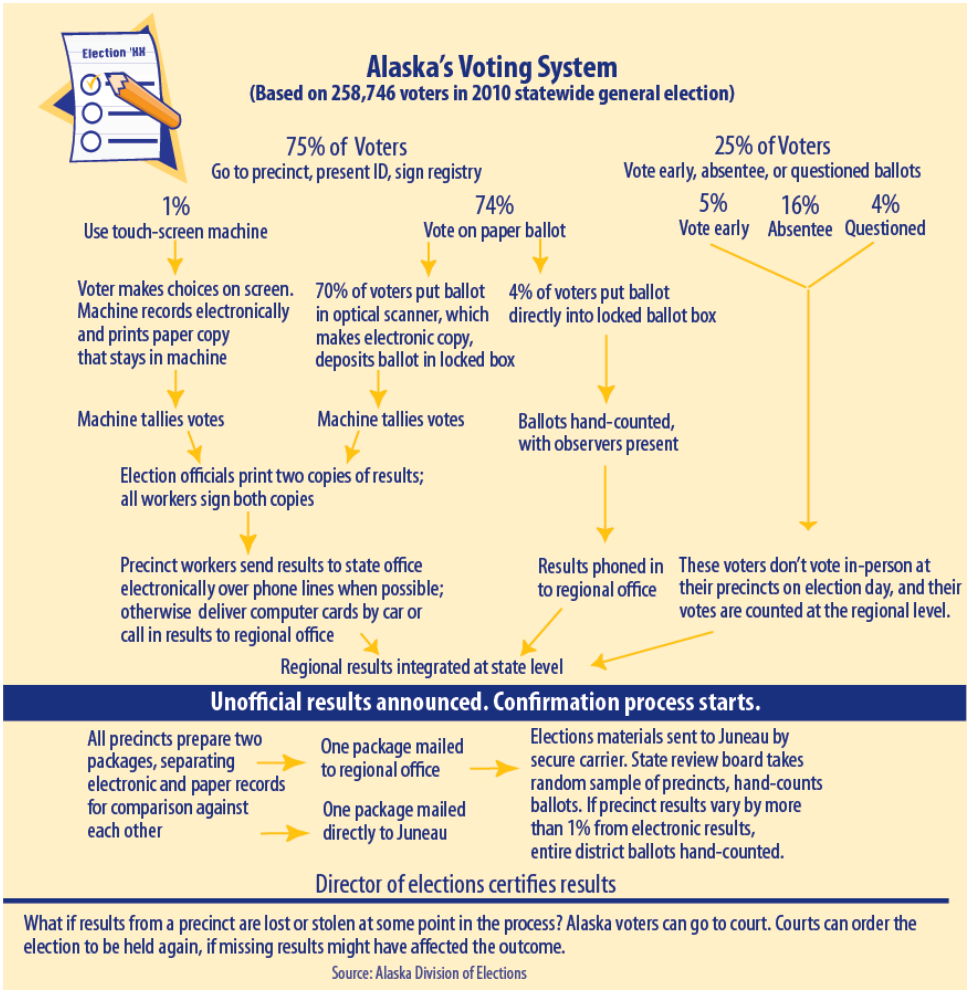
How Alaska Voters Cast Their Ballots

Alaska has many small, rural communities as well as several larger urban areas. Some of the smaller communities are not on the road system. Many of the communities are separated by large geographic distances. These characteristics influence how voters in Alaska cast their ballots. The graphic below shows that approximately 95% of Alaskans live where votes are machine counted. Approximately 5% of voters live in communities where the paper ballots are counted by hand. Regardless of how votes are counted at each of the 438 precincts in Alaska, paper ballots and electronic equipment (optical scanners and touch-screen machines) must be present on Election Day.



Alaska's Voting System

The graphic below describes Alaska's Voting System and how Alaskans choose to vote either at polling places, by voting early, by mail or fax, by absentee, or by questioned ballot. Once all of the votes have been received and counted, the final results are certified by the Director of the Division of Elections. This can sometimes take several weeks because although all mailed and absentee ballots must be postmarked on Election Day, it takes time for election workers to receive and count all of the ballots. Alaska law allows ballots to be received up to 10 days after the election if mailed within the U.S. or 15 days if mailed from international locations. All elections require great scrutiny to make sure that the results accurately reflect voter intent. This becomes even more critical in close elections.



Though Alaska's election system is among the most secure in the country, there is always room for improvement. The following summary recommendations describe and recommend opportunities to further strengthen Alaska's election system.

Equipment Security Analysis

Introduction

The State of Alaska Division of Elections Election Security Project Report (Phase 1 and 2, September 2007-May 2008) (See Appendix B) (hereto referenced as "the 2008 report") produced a comprehensive description of security enhancement recommendations. A significant portion of the 2008 report was devoted to analysis of equipment security. In the 2008 report, the State of Alaska's election system was broken into three major sections:

1. Defense in Depth
2. Fortification of Systems
3. Confidence in Outcomes

Security of the election equipment (voting machines and hardware) and the associated system software spans all three sections of the 2008 report. Among the recommendations in the 2008 report one specific item is of particular interest. The Assure 1.2 software upgrade to the voting equipment addressed a number of issues identified by third parties as significant security risks.

The State of Alaska Division of Elections has implemented all of the recommended security enhancements relating to equipment security (hardware and software systems). This includes the recently certified and adopted Assure 1.2 software revision.

Currently, no new software updates are available from the equipment vendor and considering that all of the previously recommended equipment security enhancements have been adopted no new recommendations are made in this report. One issue has been identified as a result of the Assure 1.2 upgrade. This issue is in relation to the hash code verification recommendation made in 2008. The Division of Elections adopted hash code verification of software images prior to adoption of the Assure 1.2 software. Following the adoption of the Assure 1.2 software the Division of Elections discovered that the National Software Reference Library (NSRL) did not archive the required hash code information for verification of the Assure 1.2 software integrity. Federal certification requires the Voting System Test Lab to submit the software to the NRSL. The division has reported this issue to the Election Assistance Commission (EAC). The EAC has indicated that they will get the required information to the NRSL. In the meantime, the division has received the hash code from the vendor and has verified the new software.

2008 Election Security Project Equipment Security Review

This section presents a review of recommendations made in the 2008 Division of Elections security report. Within the "Summary of Recommendations" section of the 2008 report a recommendations matrix is presented which details all of the recommended security enhancements. Listed below are the major recommendations presented in the report. A short description of each recommendation is provided as well as the current status of this recommendation within the Division of Elections.

Assure 1.2 Upgrade

The cost and process to upgrade Premier Election Solutions (formerly Diebold) system software and firmware to Assure 1.2 software version was examined. The result of this analysis determined that upon certification by the Election Assurance Commission (EAC) the Division of Elections should adopt Assure 1.2 software for all of the hardware systems within the Division: Accu-Vote Opitical Scan (AV-OS), AV-TSX and Premier Election Solutions Global Election Management Systems (GEMS).

Hash Code Verification

The GEMS.exe application should be validated by calculating both MD5 (Message-Digest 5) and SHA (Secure Hash Algorithm) hash functions. These hash codes should be compared with those registered with the National Software Reference Library (http://www.nrsl.nist.gov/votedata.html). Known vulnerabilities exist with the MD5 hash function and as a result both the MD5 and SHA hash functions should be calculated (Premier's Windows Configuration Guide, Revision 3.0, Section 10, 2007).

Password Management

A complete password management methodology was presented in the 2008 Division of Elections report. These password management recommendations encompassed all levels of the equipment ranging from system BIOS to operating system and election software passwords.

Key Card Tool

Key Card Tool is a software application created by Premier Election Systems for use with the Accu-Vote Touchscreen (AV-TSX) system. The Key Card Tool application allows users to create authentication keys and passwords on a personal computer platform and to write those authentication keys to smart cards for use in the touchscreen voting system.

Functional and Accuracy Testing

A complete set of functional and accuracy tests are provided within the 2008 report. These tests detail a set of test procedures to ensure that the voting equipment performs according to the functional requirements and that the system produces accurate tabulation results.

2011 Election Security Project Equipment Security Discussion

As discussed in the introduction to this report, the Division of Elections has adopted all of the recommended security enhancements presented in the 2008 report. This section presents the current status of these recommendations.

Assure 1.2

Current Status

In March 2011, the Division of Elections began the process to upgrade all ballot tabulation system equipment and software to Assure 1.2. The upgrade includes replacing the hardware and software in the division's eight GEMS computers, upgrading software in 510 touch screen units, upgrading software in 1,188 voter card encoders and upgrading the firmware used in the division's 356 optical scan units. The division has completed the upgrade of all equipment with the exception of optical

scan units that were used in the Fairbanks North Star Borough (FNSB) and the Kenai Peninsula Borough (KPB) October 4, 2011 municipal election. The equipment used in these areas will be upgraded to give these municipalities time to upgrade their municipal-owned GEMS computers used to program the optical scan memory cards. The division has scheduled to complete the upgrade on optical scan units used in FNSB and KPB in November 2011.

Although this upgrade provides enhanced security for the ballot tabulation system, it had an impact on the division's election results reporting. After upgrading to Assure 1.2, the division discovered that the new GEMS programming software changed how the number of precincts reporting appears on the election results reports. The election summary report, which is used to report election results, showed the number of precincts reporting for each district along with the results for each candidate. When watching election results, candidates and the public rely on the number of precincts reporting to get an indication if all precinct results have been reported.

Prior to upgrading the State of Alaska Accu-Vote system to Assure 1.2 the Division of Elections had the capability to report closed precinct statistics when a precinct uploaded the data from *either* the AV-OS or AV-TSX machines. After upgrading to Assure 1.2 a precinct was reported closed only after *both* the AV-OS and AV-TSX machines had uploaded the data to the GEMS server.

In Assure 1.2, the number of precincts reporting on the election summary report included only those precincts where **both** the optical scan and touch screen memory card were uploaded. Since optical scan memory cards are uploaded into the ballot tabulation system first, the election summary report would show results but not show the number of precincts reporting until the touch screen results were uploaded.

The reporting issue did not represent any known security risk. It could have, however, caused confusion amongst the candidates and public if they were to see results on the election summary when the number appearing in the "number of precincts reporting" section was blank because only the optical scan results had been uploaded. During the development of this report, the Division met with Dominion to discuss this issue. On March 28, 2012 this item was resolved with the vendor and the results reporting issue was fully addressed.

Recommendations

No new software revisions exist which are applicable to the State of Alaska's system. The current software (Assure 1.2) is the recommended software revision. If the current vendor of the state's election hardware develops and releases a new software version, and if this software is subsequently certified by the EAC, it is recommended that this software be analyzed for relevance to the state's system. If this analysis produces positive results it is recommended that the State adopt that new version of software.

Hash Code Verification

Current Status

Upon adopting the Assure 1.2 software version, the Division of Elections discovered that hash code verification was no longer possible using the National Software Reference Library (NSRL) website. Prior to adoption of the Assure 1.2 software the Division used the NSRL website to calculate hash codes for all software used in the system's software. After installation and commissioning of Assure 1.2 the Division of Elections discovered that the NSRL website did not contain the required hash codes.

Recommendations

It is recommended that the Division of Elections contact Dominion Voting (formally Diebold/Premier Election Systems) and investigate reasons why Assure 1.2 software hash codes have not been posted to the NSRL website. At the time of this report, the Division of Elections has received the hash code from the vendor and has verified the new software. They have also contacted EAC and reported the issue. EAC indicated that they will get the required information to the NRSL.

Password Management

No password management recommendations exist for 2011. The Division of Elections has adopted all of the recommendations from the 2008 report. No further enhancements are recommended at this time regarding password security.

Key Card Tool

Premier Election Systems Key Card Tool software was adopted in 2008 for use with the AV-TSX voting machines. No new Key Card Tool software exists and thus no new recommendations are presented in this report regarding the Key Card Tool.

Functional and Accuracy Testing

A complete set of functional and accuracy tests and procedures were presented in the 2008 report. Since an entirely new software revision has been adopted it is recommended that all of the functional and accuracy tests be revisited to ensure that the new software revision maintains all required functionality and continues to provide accurate results. Any functional tests that are no longer relevant or applicable should be removed or modified to ensure that each of the retained functional tests continue to provide useful results. Testing should be conducted to ensure that all results are accurate and are produced with the r expected format and content.

Accu-Vote Touchscreen (AV-TSX)

Argonne National Laboratory Vulnerability Assessment Team (VAT) Exploit

A man-in-the-middle exploit recently exposed by the Argonne National Laboratory Vulnerability Assessment Team (VAT) is relevant to the State of Alaska's electronic voting system. This exploit relies upon an attacker gaining access to the Accu-Vote Touchscreen (AV-TSX) voting machine in order to install a relatively inexpensive piece of custom hardware that might be used to subvert election results. The exploit presented by the Argonne National Laboratory VAT could even be installed so that remote activation is possible. The vulnerability exploits the interface between the touchscreen and the CPU of the AV-TSX machine. Information entered by the touchscreen is transferred to the CPU via the ribbon cable shown in Figure 1.

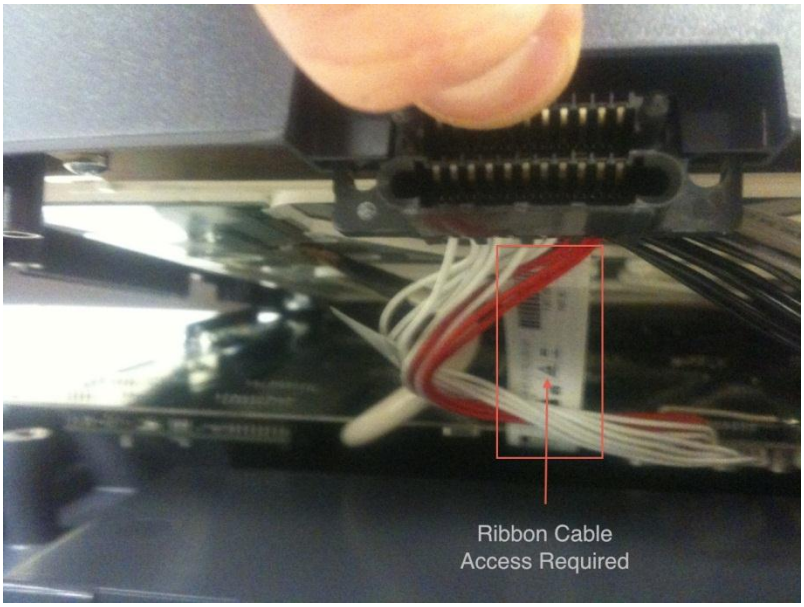


Figure 1. Touchscreen to CPU Ribbon Cable

Upon reviewing the proposed attack it is the belief of the UAA research team that the addition of two additional tamper evident machine seals would sufficiently secure the machine integrity of the AV-TSX hardware. The exploit presented relies upon gaining internal access to the AV-TSX machine.

Disassembly of the voting hardware is achieved by splitting the plastic case. Currently a serialized tamper evident seal is utilized on the top of the machine to ensure that the case is not opened without authorization. The current seal is placed across the top section of the AV-TSX unit (see Figure 2).

Figure 2. AV-TSX Current Tamper Evident Seal Location

The UAA research team was able to remove the unit screws, open the AV-TSX case and replace the screws in less than 5 minutes. The individual performing the demonstration had no prior knowledge of unit disassembly and only a simple Phillips head screwdriver was required. The unsecure nature of the AV-TSX unit in polling places requires increased security. Figure 3 shows the AV-TSX unit screw locations. Removal of these eight (8) Phillips head screws is all that is required to gain access to the interior of the AV-TSX unit.

Figure 3. AV-TSX Disassembly Screw Locations

Gaining access to the touchscreen / CPU ribbon cable does not require the current tamper evident seal to be compromised. The tamper evident seal remains intact while the rogue hardware could be installed. Figure 4 shows the touchscreen portion being lifted from the base with sufficient clearance for interior access while the tamper evident seal remains intact.

Figure 4. AV-TSX Tamper Evident Seal Integrity while Top Open

The addition of two (2) additional seals (one on each side of the case, both seals crossing the midpoint where the case is split) is required to provide sufficient security from unauthorized access since in no case would the attacker be able to open the case without cutting or damaging the seal. Figures 5 and 6 show the suggested tamper evident seal locations to ensure that unauthorized access has not occurred.

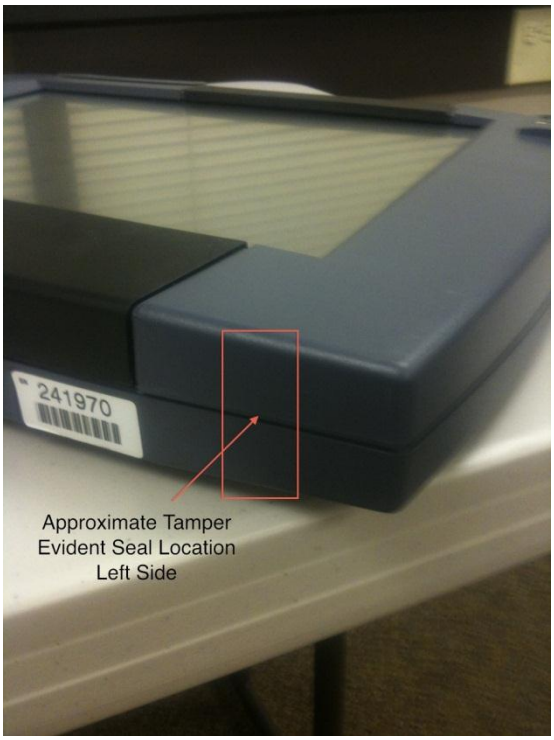


Figure 5. AV-TSX Left Side

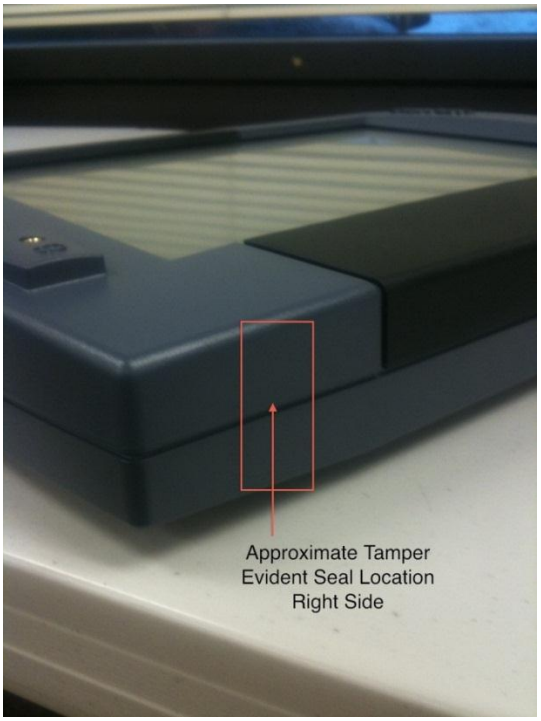


Figure 6. AV-TSX Right Side

Following the opening of the case the tamper evident seal on the top of the AV-TSX unit was inspected to ensure that the integrity of the seal was maintained. As can be seen in Figures 7 and 8, there is no evidence that the AV-TSX enclosure was opened.

Figure 7. AV-TSX Tamper Evident Seal Following Tampering (Front View)

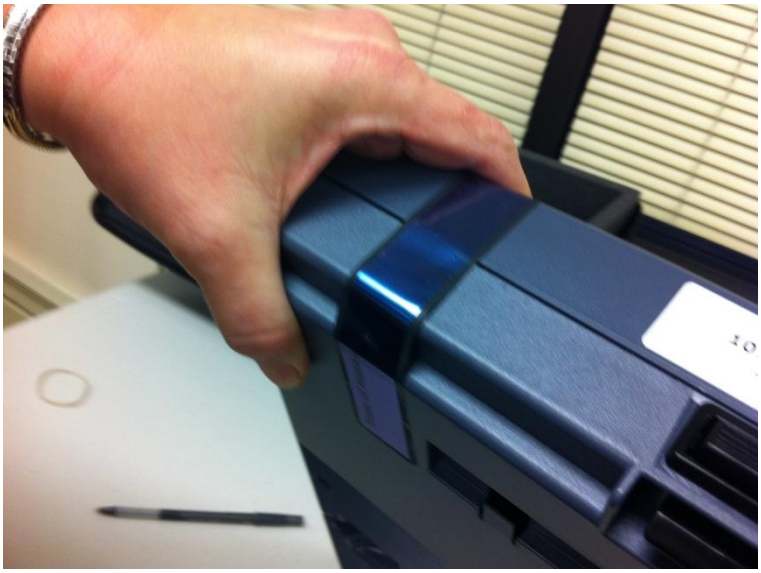


Figure 8. AV-TSX Tamper Evident Seal Following Tampering (Side View)

Serial number verification of the tamper evident seals is crucial to the success of this method. All seal serial numbers must be reviewed and logged prior to and following each election to ensure that a security breach has not occurred while the machine was in storage or while the election was in progress.

Recommendation

The Division of Elections should add two additional serialized tamper evident seals, in addition to the existing serialized tamper evident seal (for a total of three). This is the most reasonable, cost effective way to ensure AV-TSX machine security in the State of Alaska. Total election outcome security is further enhanced by the fact that the statistical use of the AV-TSX machine in elections is generally 1% or less of the total votes tallied. Thus, even if an attacker were successful in implementing the exploit (which is extremely unlikely once the tamper evident seals have been installed), the attackers ability to affect election outcomes is limited. With these additional tamper evident seals, it is highly unlikely that such an attack could occur at a polling place on Election Day or otherwise. This additional security step requires verification of seal integrity before and after the election.

End-End Ballot Security

Overview of Ballot Security

The primary issue is voting ***validity***. The election process is designed to assure that all voters' choices are correctly counted. Several basic principles serve to assure that the ballot distribution process works

correctly; beginning at the printing of the ballots to the ballots reaching the Division of Elections offices in Juneau following the election. DOE has developed procedures that are followed at all steps in the election process to assure that no eligible voters are disenfranchised, that all eligible votes are counted, that ineligible votes are not counted, and that no individual's vote is counted more than once.

A report of the process steps was originally outlined in Appendix C: The State of Alaska Election Security Project Phase 2 Report (2008) in the following sections**:**

Section 1.6 – Chain of Custody
Section 1.9 – Redundancy
Section 1.10 - Paper Ballot Tampering Vulnerabilities
Appendix F: Ballot and Election Equipment Distribution and Chain of Possession

The *accountability* and *control* of the process is addressed here along with the details regarding the specific measures taken at each step to assure validity.

LOCATION/ TRANSFER	**SECURITY MEASURES**	**RESPONSIBILITY**	**Notes**
Ballot Printer	Ballots are sequentially numbered. Ballots are shrink-wrapped in quantities of 25. Sequence numbers are recorded. Packing lists document the sequence numbers, including which ballots are contained in each box for transport.	Printer	Creates ballots printed (with sequential numbers) according to ballot requirements and specifications submitted by DOE. The Alaskan print shop has a track record of high quality ballot printing.
Contract Courier Service or Direct Delivery by Printer	The ballot printer delivers the printed ballots for the Absentee Office and Region II Office. Ballots for Fairbanks, Juneau and Nome are shipped by the printer.	Printer and Transport Company	Ballots are shrink-wrapped and sealed in transported boxes.

DOE Regional Offices	Ballot bundles are inspected and assigned for shipment to election hubs or precinct officials.	DOE Staff	Election supervisors compare each package to the ballot order to verify all sequence numbers are received and packaged correctly for the assigned precinct location as specified on master ballot order. Ballot receipt is placed with ballots for transport to election officials. Ballot bundles are inspected and assigned for shipping to election hubs or precinct officials.
Election Hubs	Precinct chairperson verifies stub numbers match ballot receipt, signs receipt and gives it to DOE. Ballot statement included in the election supplies includes the total number of ballots sent to the precinct and the stub numbers of the ballots.	Regional Election Supervisor	Anchorage, Fairbanks, Juneau, Mat-Su and Nome precincts pick up their ballots directly from DOE regional office. Ballots for all other precincts are mailed directly to precinct chairperson via USPS.
United States Postal Service (USPS)	All ballot packages are sealed and contain ballot receipt that election officials sign and return to DOE.	USPS	Ballots shipped via USPS include delivery confirmation and are sent separate from all other election materials. Ballot receipt is included with the ballots.
Election Officials	Ballots are not delivered to the polling place until election morning. Chairperson is instructed to verify ballot stub numbers against their receipt and keep ballots in secure location until being transferred to polling station. Quantity of ballots and stub numbers are also included on ballot statement that is sent to election board separately.	Precinct Election Board Chairperson	Chairperson holds ballots until Election Day.

Polling Station	After polls close, the bipartisan election board opens the ballot box and removes the voted ballots. Regular voted ballots are sealed in special tamper-evident Tyvek™ envelopes and workers are instructed to sign across the seal. Voted ballots are mailed directly from the precinct chairperson to the Director's Office in Juneau from all precincts except those delivered to hub locations or directly to a DOE office. Questioned and special needs ballots are mailed to the regional election supervisor for counting. Unused and damaged ballots are destroyed at the precincts.	Bi-Partisan precinct election board consisting of approximately 3-7 election officials.	After the poll is closed, the election board completes the ballot statement which accounts for how ballots were used. The ballot statement shows the number of voters signing the register, number of questioned ballots issued, number of special needs ballots issued and the number of spoiled ballots. Tallying (or these up provides a total number of ballots issued in each precinct. The ballot statement also includes an area where the election board records the first unused ballot stub number and the starting stub number. The starting number is subtracted from the first unused to get the total number of ballots used. The total used is then compared to the total issued to verify they match. The voted ballots are then secured for transport to the Division of Elections. (See note below)
Regional Office	The voted ballots are secured in tamper-evident Tyvek™ envelopes. Ballots from Anchorage, Mat-Su and Fairbanks are then placed in canvas transport bags that are secured with cable tie. Upon arriving at the regional office, regions complete a receiving log and give the transport bags to the secure courier who provides chain of custody documentation to DOE.	Precinct election officials, DOE Regional Offices and Secure Courier	

Secure Courier	Secure courier keeps ballots locked in alarmed area until delivered to delivery contractor. Chain of custody document maintained showing number of pieces, weight, airline moves and billing. Ballots from Wasilla are maintained with Anchorage ballots. Ballots from Fairbanks and Anchorage are placed in reserved igloo from Alaska Airlines to eliminate the possibility of being delayed. Ballots from Juneau Region I office are delivered to the Director's office. Secure contractor provides chain of custody.	Secure contractor and delivery contractor	Questioned, absentee and special needs ballots are reviewed and counted at the regional elections offices. The counted ballots are placed inside tamper-evident Tyvek™ envelopes and placed in boxes for transport by secure courier to the DOE ballot storage facility. Secure courier provides chain of custody with each delivery.

DOE Director's Office Juneau	As ballots arrive at the Director's office, DOE staff checks in each transport bag on a ballot log. The log indicates the district/precinct, precinct name and the number of voted ballot envelopes. The sealed voted ballot envelopes are then placed in labeled archive boxes in district/precinct order. The room used to store ballots is alarmed and all ballot envelopes are sealed. Access to ballot storage room is limited to authorized DOE personnel. After the election is certified, ballots used in a federal election are archived for 22 months at the State Archive location in Juneau	DOE staff	Ballots from all locations in the state are secured and stored in the DOE ballot room until archived. If a recount of ballots is held off-site, a secure contractor is hired to deliver ballots, sealed inside voted ballots envelopes and placed in archive boxes, to the counting facility. Each time ballots are removed from the storage room, a log is signed off showing which ballots were removed. When the ballots arrive at the counting location, they are verified against the log signed off when the ballots were removed from storage room. Again, the log is signed indicating all ballots arrived at counting locations. When ballots are transported from the counting location back to storage room, another log is completed and signed off before leaving the counting facility. Upon arriving back at the DOE ballot storage room, again the ballots are verified and signed off that all were transported back.

NOTE: There are 305 precincts that use an optical scan to count ballots throughout the day as the voters insert their ballot into the ballot box. When the polls close, the election board ends voting on the optical scan and the optical scan prints the election results for the precinct. The election board signs two copies of the results tape and immediately transmits results to the State's ballot tabulation system. One copy of the printed results is placed with the memory card and one copy is placed with the precinct register and ballot statement. Ballots from these precincts can be immediately sealed in the tamper-evident Tyvek™ envelopes since they have already been counted. A total of 133 precincts hand-count their ballots. The ballots from these precincts must be tallied by the bipartisan election board before being sealed in the tamper-evident Tyvek™ envelopes. The election board signs the certificate of counting on the tally book.

> The unused ballots from all precincts except Anchorage, Fairbanks, Juneau, and Wasilla are destroyed by the election board after the polls close. Unused ballots from precincts in Anchorage, Fairbanks, Juneau and Wasilla are returned to the regional office for destruction. Unused ballots in these locations are kept in secured location separate from all other materials and are destroyed after the election.

The Division of Elections carries out the election process as specified by State of Alaska Statutes, and administrative procedures are established to coordinate the control of ballots throughout the election. The challenges faced in an election are mitigated by following procedures, and relying on experienced DOE staff and volunteers who serve in several capacities as poll workers, election board members, and support staff.

As required by state statute and as established by the Division of Elections procedures for completing an election cycle, the procedure followed to keep the voting process under control has been carefully considered. These procedures were outlined in documents provided by DOE. This same procedural information is outlined in staff and volunteer training prior to Election Day.

When polls close on Election Day, 305 of 438 precincts (representing 95% of voted ballots) report their results electronically. Currently, unused ballots are either returned to regional offices along with other election material or destroyed at local precincts. The unused ballots returned to the regional offices are completely segregated from voted ballots, placed in secure storage and later shredded. The voted ballots are sent to Juneau where there is an independent validation of the electronic record (for optical scan precincts) and the register. At that point, if there is a significant difference between the number of people who voted (as recorded in the register) and the electronic tally, a “red flag” would be triggered. The stub numbers for voted ballots are recorded and certified at each precinct at the close of the election. The total number of spoiled or unused ballots is also recorded. In Juneau, the independent validation of the registry (number of people who voted), the actual number of paper ballots, and the electronic record are independently verified and then compared for accuracy. A similar “red flag” would be triggered if a significant number of ballots were used and scanned compared to the actual number of voters in an optical scan district, or if a hand-count precinct (133 precincts representing 5% of voted ballots) recorded a significant discrepancy between the number of voted ballots and the number of ballots used (ballots either voted or spoiled).

In hand-count precincts, the entire bi-partisan precinct board would have to work in collusion in order to replace voted ballots with fraudulently marked “unused” ballots and to falsify the ballot statement. The independent verification of the election material (registry, voted paper ballots, and ballot statement) in Juneau would likely reveal any such discrepancies, and would prompt further scrutiny and action.

Returning all unvoted ballots to Juneau could eliminate this risk, however, since all voted ballots are also returned to Juneau, new risks might be introduced by having all voted and unused ballots in the same location. In addition to security risks that could result from returning all unused ballots to Juneau, it is also very costly (transportation and storage).

Recommendations

The voted ballots are handled as outlined in this section with the chain of possession and responsibilities as described. Currently, the unused and spoiled ballots at the remote polling locations are destroyed as part of the procedures after the polls are closed. Unused ballots from optical scan precincts in Anchorage, Fairbanks, Juneau and Wasilla are returned to the regional office where they are segregated from voted ballots and destroyed. Because the unused ballots in these locations are kept in secured locations separate from all other materials and are destroyed after the election, there is no chance that they can re-enter the election process.

There is little risk of ballot tampering because there are duplicate and independent tallies of the results from the voting machines and the transmitted results. Any subsequent discrepancies would be a "red flag" regarding the counts. In the case of the 133 precincts where the voting is compiled by hand-count, the immediate tally is also transmitted by phone to preclude any changes occurring.

In order to further secure the unvoted ballots and mitigate the risk of fraudulently marked unvoted ballots entering the election system, we recommend that the full board of election officials in optical scan precincts record, certify and sign-off the remaining unused and spoiled ballot stub numbers and secure the unused and spoiled ballots in boxes with tamper evident seals **BEFORE** the voted ballot boxes are opened. Further, the precincts should seal the boxes of unvoted/spoiled ballots with tamper evident seals prior to returning them to the regional offices. If a precinct attempts to deliver unused ballots to the regional office in an unsealed box, the regional office election staff should require them to account for the unused ballots and seal the box. Those sealed boxes returned to the regional offices will then be transferred to an external agency (e.g., Shred Alaska) for destruction. In hand count precincts we recommend that the unused and spoiled ballot stub numbers be recorded, certified and signed off by the full precinct board, and the unvoted/spoiled ballots be destroyed before opening the voted ballot box. This additional recording, certification, and sign-off of the ballot statement, including the unvoted and spoiled ballots, will add the same level of formality and accountability for unvoted and spoiled ballots as for voted ballots. This action will cause a short delay in counting voted ballots, but will improve the security of the process The Division of Elections should include these instructions in training materials, procedures and checklists for poll workers prior to and on Election Day.

In both optical scan and hand-count precincts, the unused/spoiled ballots should be processed or destroyed prior to opening the voted ballot boxes. This additional step will ensure that no fraudulently completed or spoiled ballots can become comingled with or replace secured voted ballots.

Further, we recommend that the division also seal (using tamper evident tape) the “banker boxes” that are used to transport the sealed voted ballot packages within the Juneau office for further hand-count verification. This step would ensure that no inadvertent packages of voted ballots could be inserted into the boxes. The seal for the box and the subsequent seals of the envelopes inside could be broken under appropriate supervision at the proper point in the hand-count verification process.

Post-election Audit and Hand Count Procedures

The purpose of the post-election audits is to verify results and maintain public trust. Audits do this by independently verifying that the machine counts were correct and confirming that a manual recount would not change the outcome. In the following section, we describe the process for counting absentee, questioned, and early vote ballots. We also discuss the role of the State Review Board and the hand-count verification process in validating election results.

Absentee and Early Voting

Absentee voting is a major component of the election process. In the 2010 general election, 21% of voters voted absentee or early ballots [1]. There are two broad categories of absentee voting. The first category includes absentee by mail, fax, and special advanced requests. The second category is called "in-person absentee." It includes special needs voting, early voting, and absentee in person voting.

Absentee and early voting can begin 15 days prior to Election Day. Absentee and early ballots are issued at the house district level, not at the precinct level because the division's existing voter registration and election management (VREMS) database is programmed and designed to track absentee and early ballots by house district. The division does not use voting equipment in absentee polling locations.

When the regional office receives voted absentee ballots, they record the daily total on a spreadsheet. Regional staff record that a voted ballot was received on each voter's record in VREMS. Each ballot entered is assigned a sequence number. A count report is produced from VREMS showing the total number of ballots entered. After ballots are logged into VREMS, the bipartisan Absentee Ballot Review Board (ARB) reviews the ballots and records on their audit logs the number of ballots reviewed and the type of count (full count, partial count, or rejected ballot). The voted ballots that are eligible for counting are given to the Regional Accu-Vote Board (RAB) for counting and inclusion into the election results.

Before the ARB begins to count absentee and early ballots, the division conducts a duplicate analysis to verify that the voter did not vote more than once. The division cannot conduct the duplicate analysis until they have updated all voter history from the precinct registers used in the polling places. Once the division has manually updated all voter history, they can begin to open and count the absentee ballots. AS 15.20.201 requires that all absentee ballots be reviewed, opened, and counted by the 15th day after the election.

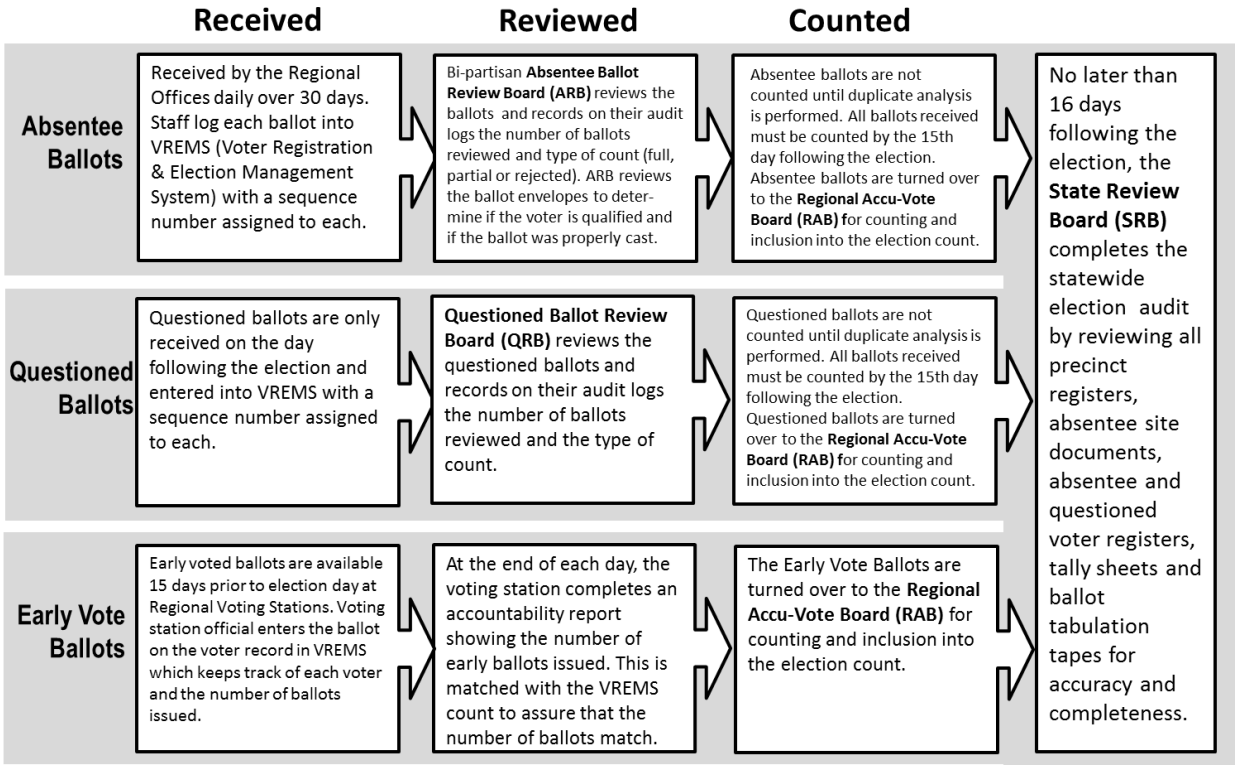
Having this system to manage absentee and early ballots by house district allows the division to verify that the number of ballots accepted for counting matches the number of actual ballots reported in the election results. This is critical to the integrity of the ballot accountability process.

[1] 258,746 people voted in the 2010 General Election. Of these, 192,978 voted in-person at the polling place in their precinct; 40,834(16%) voted an absentee ballot; 13,246(5%) voted an early ballot; and 11,688 (4%) voted a questioned ballot.

Accounting for Absentee/Questioned Ballots

Ensuring that all absentee, questioned, and early voted ballots are counted is a three part process—receive, review, and count. Each step is performed independently to provide a check and balance which ensures that all ballots are accounted for.

Summary of Absentee, Questioned and Early Voting Ballot Checks



Each of the four regional offices receives voted ballots from their region. Absentee ballots can be received daily before an election through the 15th day following Election Day. The daily total is recorded on a spreadsheet. Questioned ballots are only received one time (after Election Day) and are recorded on the audit log. The total number of ballots received is verified by the Questioned Ballot Review Board (QRB).

Regional election staff enter that a voted ballot was received into each voter's record in the division's voter registration and election management system (VREMS). Each ballot entered is assigned a sequence number. A count report is produced from VREMS showing the total number of ballots entered for both absentee and questioned ballots.

After ballots are logged into VREMS, the bipartisan QRB and Absentee Ballot Review Board (ARB) review the ballots and record on their audit logs the number of ballots reviewed and type of count (full count, partial count, or rejected ballots). Each of these processes—VREMS and the audit logs—produce independent results that can be compared to assure that the number of ballots voted is the same as the number reviewed.

The voted ballots that are eligible for counting are given to the Regional Accu-Vote Board (RAB) for counting and inclusion into the election results. The election results are then sent to the State Review Board (SRB) along with all the other election materials so that the board can complete the statewide election audit.

Review Boards

The integrity of post-election procedures is established when all the independent processes come together and balance. To ensure the integrity of the system, the State of Alaska by statute has provided for bipartisan review boards at both the regional and state level. The ARB, QRB and the RAB operate at the regional level. The SRB in Juneau is the final check prior to certification of the election. In addition to auditing the paper ballots and the electronic counts, the SRB conducts hand-count verifications for each of the forty House districts to make sure that the election results are correct. We describe these review boards and hand-count verification procedure below. Together they establish that the election is verifiable and that the public can be confident of the outcome.

Absentee Ballot and Questioned Ballot Review Boards

Thirty days before the election, each regional election supervisor appoints an ARB and a QRB for each district in the region. Under AS 15.20.190, each board must be composed of at least four members. The board members work in bi-partisan teams of two when reviewing ballots. Team members must be from different political affiliations. Each team will review ballots one district at a time. The teams review ballots using the absentee ballot register or the questioned ballot register. During the review process, observers who represent a candidate or a ballot issue may be present. Ballot review begins seven days before Election Day for absentee ballots, and two days after Election Day for questioned ballots. Counting of the questioned and absentee ballots that have been reviewed begins after Election Day as soon as election workers have updated the voter registration records and completed their duplicate analysis to ensure that no one has cast more than one vote. All ballots received must be reviewed and counted by the 15th day following the election (AS 15.20.201).

The review board is responsible for the following:

- Verifying ballots are stored in a secure location with limited access.
- Reviewing each voted ballot envelope to determine whether the voter is qualified to vote and if the ballot was properly cast.
- Verifying that the appropriate accept or reject code has been assigned to the ballot and that there is a ballot envelope for each voter appearing on the absentee ballot register.
- Maintaining ballot accountability and verifying that the number of ballots received equals the number of ballots reviewed and counted. Each ballot entered into VREMS must be accounted for.

In addition to the absentee and questioned ballots, there are early voted ballots in each region. Early voted ballots are issued beginning 15 days prior to the election at the Regional Voting Station. At the time of voting, the voting station official enters the ballot on the voter record in VREMS. VREMS keeps track of each voter and the number of ballots issued.

At the end of each day, the voting station completes an absentee ballot accountability report showing the number of early ballots issued. The accountability report is compared to the VREMS early vote count report to make sure the number of ballots match.

When the voting period is over, a final VREMS report is printed showing the number of early ballots received. The early voted ballots are then given to the Regional Accu-Vote Board for counting and inclusion into the elections results.

Regional Accu-Vote Board

The election supervisor in each region also appoints a bipartisan Regional Accu-Vote Review Board (RAB) made up of no more than eight members. No more than two members may be of the same political party. The RAB is responsible for overseeing the counting of absentee and questioned ballots and for assisting the division in pre-election processes. (6 AAC 25.030)

The voted ballots that are eligible for counting in each region are given to the Regional Accu-Vote Boards for counting and inclusion into the election results.

State Review Board

The director of the division appoints the State Review Board (SRB) at least 30 days before the election. Alaska statutes require the director to review the counting of the ballots with the assistance of and in the presence of the appointed representatives from the political parties. The State Review Board (SRB) is a bipartisan review board made up of at least 8 members for primary and general elections, and at least 4-6 members for state conducted local elections. The SRB is responsible for testing the ballot count programming prior to the election. No later than 16 days after the election, the SRB is required to review all precinct registers, absentee site documentation, absentee and questioned voter registers, tally sheets, and ballot tabulation tapes to ensure that reported election returns are accurate and complete. AS 15.15.420-450.

Completing the audit of statewide election returns involves a review and comparison of the election results reported on the district statement of votes cast (SOVC) report printed from GEMS with the information provided on precinct registers, absentee documents, questioned registers, tally sheets, and other materials to assure that they are accurate.

Prior to certifying the election the SRB also conducts a hand-count verification in at least one precinct in each of the 40 districts in the state. The selected precinct must account for at least 5% of the ballots voted in that district.

Hand-count Verification Process – Additional Requirement for Verification

In 2005 the Alaska Legislature—in response to the heightened public scrutiny of electronic voting and the passage of the Help America Vote Act (HAVA)—set out the procedure for the hand-count verification

process in AS 15.15.30.[2] Hand-count verification is performed on one randomly selected precinct in each of the 40 house districts. The precinct selected must account for at least 5% of the votes cast in the district as reported election night. This requirement ensures that the selected sample size is large enough to be statistically significant but not so large that hand-counting votes delays certification of election results.

Election workers determine which precincts in each district represent 5% of ballots cast in that district. DOE staff then writes the numbers of the qualifying precincts on pieces of paper and put these in envelopes by district. Two bi-partisan SRB review board members select the random sample by drawing a precinct for each district. The ballots in the selected precincts are then hand-counted by about 40 election workers. If there is a discrepancy of greater than 1%, the entire district is recounted by hand. There has never been a discrepancy of 1% during the 6 years that this statute has been in effect. All the discrepancies that the division has found have been caused by marginally marked ballots. If a voter does not completely fill in an oval on the ballot, the optical scan machine at the election precincts might not detect the vote on Election Day. This is why the Division of Elections reminds voters in the voting booth to completely fill in the oval in order to make sure that their vote is counted.

Alaska began hand-counting ballots for these audits in 2006, shortly after the legislature unanimously passed H.B. 459 and signed it into law (2005). At that time, Alaska was only the sixth state in the nation to commit to using the manual audit. In 2008, at the time of the last report, Alaska was one of only 12 states (Norden 2007) to routinely conduct post-election manual audits to verify whether electronic and mechanical voting equipment was properly counting, recording, and storing voting information. In 2011, according to the Verified Voting Foundation (www.verifiedvoting.org), there are at least 21 states that have passed similar legislation requiring post-election manual hand counts of voter-verified paper records (VVPR) for their audits. But not all audits work like Alaska's. Some states sample 1% of all precincts. In Florida, the audit follows election certification, and some states randomly select a larger proportion of precincts, but only audit one result. California has plans to test alternative sample size and audit methodologies but it is uncertain when that research will take place and if the results would have any applicability in a small population state like Alaska.

It is important to take into account the unique characteristics of Alaska when comparing it to other states. Alaska has a statewide election system and a small and geographically diverse population. When the Alaska legislature included the current sampling system in the Alaska statutes, they balanced the importance of having a sample size large enough to detect any potential error in the ballot count with the practical consideration of not hand-counting so many votes that the verification procedure would unduly delay certification of elections results.

The current system reflects the intent of the legislature and ensures that Alaska's random selection process is transparent since observers only need to go to one place to witness the audit by the State

[2] Prior to the passage of AS 15.15.430 in 2005, the Division of Elections had been hand-counting votes to verify electronic counts in races where a recount was required. These recounts never demonstrated a discrepancy of 1% and the discrepancies were always because of marginally marked ballots.

Review Board. Current reported research, along with the fact that there has never been a discrepancy of 1% since the statute has been in effect, indicates that the current system is working.

Precinct Election Boards

Precinct Election Boards are the core of the electoral process. The regional supervisors begin recruiting election workers to serve on bipartisan precinct election boards around March of every election year. The election supervisor appoints a chairperson for each board, and the chairperson then helps the division to recruit registered voters to serve on the precinct board. AS 15.10.120. The precinct board usually consists of about 3 to 7 election workers.

Election worker recruitment is one of the more time consuming tasks in conducting a successful election. There is a precinct election board for each of the 438 precincts in the state. As part of the recruitment process, the division notifies the political parties that they are eligible to nominate election workers for each precinct election board. These nominations must be made by April 15th of an election year. The election supervisor appoints one nominee from the governor's political party and one from the party that received the second highest number of votes in the last statewide election.

Political parties do not always nominate election board members for every precinct. In the 2010 election, there were occasions when a board was composed entirely of non-affiliated election workers.

Precinct election board members attend regional training offered by the Division of Election before Election Day. On Election Day, they operate the polling place. This includes setting up equipment, assisting voters, checking voter identification, making sure voter's sign the voter register, and ensuring that ballots are confidential and voters have placed their ballots in the optical scan machines or the ballot box. After the polls close, these election workers are also responsible for counting ballots in hand-count precincts. All precinct workers must be sure that all ballots and registers are returned to their regional office on election night.

Real-time Voter History Solutions Descriptions and Evaluation (See Appendix E: Real-time Voter History Solution Evaluation)

Voter Eligibility

Eligible Voters

Article V of the Alaska Constitution gives every citizen of the United States, who is 18 years old and has registered to vote in Alaska at least 30 days before an election, the right to vote in any state or local election. Qualification and registration of voters is further described in AS 15.05.010-15.07.200.

Ineligible Voters

The division's responsibility under the law is to enfranchise voters and make sure that their vote counts. If the person's name is on the Voter Registry, he or she is allowed to vote. If there is a doubt with regard to eligibility, they will be asked to vote a questioned ballot and the reason will be written on the ballot envelope. The division has no authority to question voters' statements on voter registrations and no enforcement powers. In addition, all data matching and investigations require additional funding and staffing so the division must be sure that the results of such investigations are worth the time and funding.

Felons

A person convicted of a crime that is considered a felony involving moral turpitude under state or federal law may not vote unless he or she has completed the sentence, including probation or parole (AS 15.05.030). Alaska's restriction on voters with felony convictions is not a lifetime ban. Any person who is unconditionally discharged, can re-register to vote. The division is required to make reasonable efforts to obtain names of convicted persons. (AS 15.07.135(b)).

The division has a process in place to remove voters that have been convicted of a felony involving moral turpitude. According to Alaska statute, nearly all felonies involve moral turpitude.[3] The Division regularly receives electronic information from the Alaska Corrections Offender Management System (ACOMS) relating to convicted state felons. Using the ACOMS data, DOE staff matches offenders on the ACOMS list with voter registration files. If a registered voter is convicted of a felony involving moral turpitude, the division inactivates the voter registration record. When the courts unconditionally discharge a felon following completion of a sentence, the division and the voter receive a Notification of Restoration of Voting Rights. The division indicates on the voter registration record that the voter has been discharged and the voter is then eligible to re-register to vote.

The division matches ACOMS and voter registration data, at a minimum, on a monthly basis. The most difficult time to perform this match is immediately prior to generating the precinct registers needed to conduct an election. Registers must be created approximately three weeks prior to an election so the division has time to distribute the paper registers throughout the state. Since registration activity is the highest at the 30-day registration deadline for an election, staff resources are busy with processing

[3] "Felonies involving moral turpitude" include those crimes that are immoral or wrong in themselves such as murder, manslaughter, assault, sexual assault, sexual abuse of a minor, unlawful exploitation of a minor, robbery, extortion, coercion, kidnapping, incest, arson, burglary, theft, forgery, criminal possession of a forgery device, offering a false instrument for recording, scheme to defraud, falsifying business records, commercial bribe receiving, commercial bribery, bribery, receiving a bribe, perjury, perjury by inconsistent statements, endangering the welfare of a minor, escape, promoting contraband, interference with official proceedings, receiving a bribe by a witness or a juror, jury tampering, misconduct by a juror, tampering with physical evidence, hindering prosecution, terroristic threatening, riot, criminal possession of explosives, unlawful furnishing of explosives, promoting prostitution, criminal mischief, misconduct involving a controlled substance or an imitation controlled substance, permitting an escape, promoting gambling, possession of gambling records, distribution of child pornography, and possession of child pornography.

registration applications received on or before the registration deadline so registers can be created. If the felon list from ACOMS is not processed immediately prior to the registers being created, or if a person is convicted of a felony between the time the register is created and Election Day, there is a possibility that convicted felons could appear on the register and vote. However, nearly all felons convicted of crimes of moral turpitude are incarcerated following their conviction and are not available to vote.

Although there is a possibility for a convicted felon to appear on the register if the person was convicted in the timeframe after the register is created and before Election Day, the number of potential felons is quite low compared to the statewide number of registered voters. In 2010, on average, the division inactivated approximately 25 registered voters each time the ACOMS list was matched with the statewide registration database. By processing the ACOMS list immediately before generating registers, the number of potential state felons that appear on the register and have the opportunity to vote is less than .005%.

In addition to the ACOMS list, the division receives notices of federal felony convictions from the U.S. District Court. Like the ACOMS list, the division looks up each name on the federal felon list in the statewide registration database to determine if the person is a registered voter. If the person is a registered voter, the division inactivates the record if the person is convicted of a federal felony involving moral turpitude. However, the division does not have direct access to the federal felon database so must rely upon the federal court staff to provide the notices.

The division is dependent upon the ACOMS data provided by the Division of Corrections and information provided by the U.S. District Court when staff removes felons from the voter registration rolls. If the data provided to the division is current and accurate, and the division processes the data quickly and before the precinct registers are created, the probability that a convicted felon remains registered and votes is very low.

Recommendations

Division procedures are adequate to prevent felons convicted of crimes of moral turpitude from voting. The division should continue their efforts to strengthen integration of data sources with state and federal courts and the Department of Corrections.

Non-U.S. Citizens

Alaska requires a prospective voter to sign an affidavit attesting to his or her citizenship in the United States. When a voter registers to vote before a registrar, they must show identification. If no identification is provided, the registrar notes on the registration form that no ID was presented. When the division processes this form, the voter's identity is verified through the Division of Motor Vehicles (DMV) database and/or through a direct application between DMV and the Social Security Administration (SSA). When a voter registers to vote by mail, their identity is also verified through these databases.

If the identity of a voter cannot be verified through either the DMV or SSA databases, the division makes a notation next to the voter's name on the precinct register that the voter must show identification. A voter who is personally known by an election worker cannot have the identification requirement waived if this notation is next to the voter's name on the precinct register.

If the division receives information that a voter is not qualified because they are not a U.S. citizen, the division requests verification of U.S. citizenship through the voter and/or the Immigration and Naturalization Service. If it is found that the voter is not a U.S. citizen, the division will inactivate the voter registration record.

Federal law—the National Voter Registration Act—allows voters to register without documentation but stipulates that lying about citizenship is perjury.

In Alaska you can get a driver's license or a Permanent Fund Dividend (PFD) without being a United States citizen. You are encouraged to register to vote at the Department of Motor Vehicles and so occasionally a non-U.S. citizen does register to vote there. The PFD application asks you if you are a U.S citizen. The division now has an agreement with the Department of Revenue to match data with the PFD database to determine if a voter has declared that he or she is not a U.S. citizen on the PFD application.

In 2011, the division did a data match of the PFD database and the statewide voter registration list to ensure that the voter rolls contained only the names of eligible voters. Out of 487,162 registered voters, the division found only 380 individuals who marked on the PFD application that they were not U.S. citizens. The division mailed a letter to all PFD applicants who indicated they were not U.s, citizens on their application form. The divisions included a cancellation form with the letter so the applicant could cancel his voter registration if he was not a citizen. As of September 28, 2011, the division has received 153 responses from voters confirming that they are U.S. citizens. Many stated that they became citizens after they applied for the PFD. Seventy-five people responded that they were not U.S. citizens and requested that their voter registration be cancelled.

The division also has an agreement with the U.S. Immigration and Naturalization Service in Alaska to receive names from INS once an immigration case is concluded. The division then sends those voters a notice telling them they may not vote if they are not U.S. citizens.

In addition, the division provides the Alaska Voter Registry to the federal courts for jury selection. If jurors say they are not U.S. citizens in their response to a notice of jury duty, the court will send their name to the division of elections and the division will contact them to confirm their status.

Other Ineligible Voters

The division currently matches voter registration lists with the state of Washington to see if there are duplicates. The division then writes to the voters to tell them that they are registered in both states and to ask them to notify the Alaska Division of Elections if they no longer wish to be registered to vote in Alaska. The last time the division did a match, 65.7% of the identified voters wrote back to cancel their registrations. The Division also performed a similar match with the State of Oregon and sent a notice to

voters registered in both states. 65.6% of the voters notified in the Oregon match responded to cancel their registrations.

The division actively looks for information on deceased voters. They receive a monthly list from the Alaska Bureau of Vital Statistics. Staff members check obituaries every day and also receive notifications from family members and election workers. The national Social Security database is so large that it is impractical for the division to match it with their Voter Registry.

Poll Worker Training

Poll worker training was not included in the scope of work for this report.

Confidence in Outcomes

Division processes for handling public comment are not included in the scope of work for this report.

Summary Recommendations

Equipment Security

Assure 1.2

No new software revisions exist which are applicable to the State of Alaska's system. The current software (Assure 1.2) is the recommended software revision. If the current vendor of the state's election hardware develops and releases a new software version, and if this software is subsequently certified by the EAC, it is recommended that this software be analyzed for relevance to the state's system. If this analysis produces positive results it is recommended that the State adopt that new version of software.

Hash code Verification

It is recommended that the Division of Elections contact Dominion Voting (formally Diebold/Premier Election Systems) and investigate reasons why Assure 1.2 software hash codes have not been posted to the NSRL website. At the time of this report, the Division of Elections has received the hash code from the vendor and has verified the new software. They have also contacted EAC and reported the issue. EAC indicated that they will get the required information to the NRSL.

AV-TSX Touchscreen System Tamper Evident Seals

The Division of Elections should add two additional serialized tamper evident seals, in addition to the existing serialized tamper evident seal (for a total of three), is the most reasonable, cost effective way to ensure AV-TSX machine security in the State of Alaska. Total election outcome security is further enhanced by the fact that the statistical use of the AV-TSX machine in elections is generally 1% or less of the total votes tallied. Thus, even if an attacker were successful in implementing the exploit (which is extremely unlikely once the tamper evident seals have been installed), the attackers ability to affect election outcomes is limited.

End-End Ballot Security

The voted ballots are handled as outlined in that section of this document with the chain of possession and responsibilities as described. Currently, the unused and spoiled ballots at the remote polling locations are destroyed as part of the procedures after the polls are closed. Unused ballots from optical scan precincts in Anchorage, Fairbanks, Juneau and Wasilla are returned to the regional office where they are segregated from voted ballots and destroyed. Because the unused ballots in these locations are kept in secured locations separate from all other materials and are destroyed after the election, there is no chance that they can re-enter the election process.

There is little risk of ballot tampering because there are duplicate and independent tallies of the results from the voting machines and the transmitted results. Any subsequent discrepancies would be a "red flag" regarding the counts. In the case of the 133 precincts where the voting is compiled by hand-count, the immediate tally is also transmitted by phone to preclude any changes occurring.

In order to further secure the unvoted ballots and mitigate the risk of fraudulently marked unvoted ballots entering the election system, we recommend that the full board of election officials in optical scan precincts record, certify and sign-off the remaining unused and spoiled ballot stub numbers and secure the unused and spoiled ballots in boxes with tamper evident seals **BEFORE** the voted ballot boxes are opened. Further, the precincts should seal the boxes of unvoted/spoiled ballots with tamper evident seals prior to returning them to the regional offices. If a precinct attempts to deliver unused ballots to the regional office in an unsealed box, the regional office election staff should require them to account for the unused ballots and seal the box. Those sealed boxes returned to the regional offices should then be transferred to an external agency (e.g., Shred Alaska) for final destruction. In hand count precincts we recommend that the unused and spoiled ballot stub numbers be recorded, certified and signed off by the full precinct board, and the unvoted/spoiled ballots be destroyed before opening the voted ballot box. This additional recording, certification, and sign-off of the ballot statement, including the unvoted and spoiled ballots, will add the same level of formality and accountability for unvoted and spoiled ballots as for voted ballots. This action will cause a short delay in counting voted ballots, but will improve the security of the process The Division of Elections should include these instructions in training materials, procedures and checklists for poll workers prior to and on Election Day.

In both optical scan and hand-count precincts, the unused/spoiled ballots should be processed or destroyed prior to opening the voted ballot boxes. This additional step will ensure that no fraudulently completed or spoiled ballots can become comingled with or replace secured voted ballots.

Further, we recommend that the division also seal (using tamper evident tape) the “banker boxes” that are used to transport the sealed voted ballot packages within the Juneau office for further hand-count verification. This step would ensure that no inadvertent packages of voted ballots could be inserted into the boxes. The seal for the box and the subsequent seals of the envelopes inside could be broken under appropriate supervision at the proper point in the hand-count verification process.

Real-time Voter History Solutions (See Appendix E: Real-time Voter History Solution Evaluation)

Voter Eligibility

Division procedures are adequate to prevent felons convicted of crimes of moral turpitude from voting. The division should continue their efforts to strengthen integration of data sources with state and federal courts and the Department of Corrections.

Election Process Auditability Checklist

Maintain a comprehensive election auditability checklist before, during, and after each election to demonstrate that all election procedures have been implemented and have been reviewed by the proper level of authority. An example of this checklist can be found in Appendix F: Election Process Auditability Checklist.

Recommendations for Future Study

The team recommends that the Division of Elections conduct a study to develop a comprehensive long-term electronic voting strategy for Alaska including a phased migration from existing equipment to newer technologies and platforms. In the context of that longer term strategy, the Division should further evaluate the benefits of epollbook solutions including RTVH capabilities. In order to ensure that Alaska continues to provide a secure, participative, and effective election system into the future, this this research could also explore the implications of emerging technologies on current election processes, evolving security risks, voter participation and perception, as well as the impacts on recruitment and training of future election officials and poll workers.

Appendices

State of Alaska
Election Security Project:
Election Process Review
Phase 3 Report

Appendix A: Glossary of Acronyms in Report

Appendix A

Glossary of Acronyms in Report

AAC	Alaska Administrative Code
ACOMS	Alaska Corrections Offender Management System
ARB	Absentee Ballot Review Board
AS	Alaska Statue
AV-TSX	AccuVote Touchscreen system
AV-OS	AccuVote Optical Scan
BIOS	Basic Input/Output System
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
DMV	Division of Motor Vehicles
DOE	Division of Elections
EA	Election Administrators (vendor)
EAC	Election Assistance Commission
EPB	Electronic Poll Books
ES&S	Election Systems and Software (vendor)
EViD	Election Voter Identification (product)
FNSB	Fairbanks North Star Borough
GEMS	Premier Election Solutions Global Election Management Systems
HAVA	Help America Vote Act
H.B.	House Bill
KPB	Kenai Peninsula Borough
MD5	Message-Digest 5 hash functions
NSRL	National Software Reference Library
PC	Personal Computer
PFD	Alaska Permanent Fund Dividend
QR	Quick Response scan code
QRB	Questioned Ballot Review Board
RAB	Regional Accu-Vote Board
REAA	Regional Educational Attendance Area elections
RTVH	Real Time Voter History
SHA	Secure Hash Algorithm
SOVC	Statement of Votes Cast
SRB	State Ballot Counting Review Board
SSA	Social Security Administration
UAA	University of Alaska Anchorage
US	United States
U.S.	United States
USPS	United States Postal Service
VAT	Argonne National Laboratory Vulnerability Assessment Team
VOTEC	(Not an Acronym, vendor's name)
VREMS	Voter Registration and Election Management System
VR Systems	(Not an Acronym, vendor's name)
VVPR	Voter-Verified Paper Records

State of Alaska
Election Security Project:
Election Process Review
Phase 3 Report

Appendix B: 2010 General Election Review
(April 1, 2010)

State of Alaska

Office of Lieutenant Governor Mead Treadwell

2010 General Election Review

April 1, 2011

2010 General Election Review
Office of Lieutenant Governor Mead Treadwell
Table of Contents

2010 General Election Review
Executive Summary
Office of Lieutenant Governor Mead Treadwell

In December 2010, after Governor Sean Parnell and Lieutenant Governor Mead Treadwell signed final paperwork to certify the 2010 United States Senate election, the Lt. Governor announced he would conduct a review of the state's election procedures and statutes. The historic write-in campaign by Senator Lisa Murkowski revealed sections of election law and procedures that were yet untested, and many Alaskans became more aware of election procedures.

The following 2010 Election Review report by the Office of the Lieutenant Governor, the Division of Elections and the Department of Law, includes an analysis of election law and procedures as well as feedback from stakeholders, political parties, and most importantly, Alaska's voters. The report responds to observations and concerns made by Alaskans, and offers a recommendation for change or retraction of current procedures, Alaska State Statute and or regulation for each issue.

A key change recommended as a result of this review is intended to make it easier for Alaskans serving in the military to vote. Those recommendations include changing the date of the primary to make sure ballots for a general election can be in the mail in time for service members overseas, allowing other electronic forms of transmission – besides faxes – of ballots back to Alaska, and working with the Redistricting Board and the Department of Defense to facilitate reopening of polling places on Alaska's military bases.

Other key recommendations include changes to state law to clarify procedures for counting write-in ballots and making the declaration of candidacy for a write-in candidate voluntary. Perhaps the single most important finding in the review is that no change in procedure or state law recommended would have changed the outcome of the 2010 General Election.

Our heartfelt thanks goes out to those who worked so tirelessly on the 2010 General Election, including former Lieutenant Governor Craig Campbell, division personnel, attorneys from the Department of Law, candidates, and especially the volunteers who so selflessly gave their time and energy to bring the election to a conclusion. And thanks are due to Alaskans for taking their time to submit comments, to stakeholders for meeting with the Lieutenant Governor, and to the Division of Elections, with special thanks to Director Gail Fenumiai, and Department of Law for their assistance in this review.

The following is a summary of the recommendations detailed in the full report:

Recommended amendments to Alaska State Statute:

- Amend Alaska State Statute to allow a U.S. citizen, 18 years or older, who has never been a resident of another state, to register to vote in Alaska so long as the child's parent is eligible to register and vote in Alaska.

- Amend Alaska State Statute to add a new subsection clarifying the rules for counting write-in votes, and allowing the director of elections to disregard misspellings or other minor

variations in the form of a candidate's name if the intention of the voter can be ascertained. This change would have Alaska law conform to recent Supreme Court rulings on voter intent.

- Amend Alaska State Statute to add a new section setting out the process for counting write-in votes. This information is currently set out in regulation.

- Amend Alaska State Statute to extend the time a voter may apply to an election supervisor for an absentee ballot to the 22nd day before the election rather than the 15th day.

- Amend Alaska State Statute to extend the time for early voting to 22 days before an election, rather than 15 days.

- Amend Alaska State Statute to allow an absent uniformed services voter or an overseas voter to apply to vote by electronic transmission any time during the calendar year, and to return the ballot in a manner established by the director in regulation.

- Amend Alaska State Statute to allow the director to establish in regulation the method of electronic transmission for delivery of an absentee ballot by electronic transmission. This would allow receipt of ballots by electronic means other than fax.

- Amend Alaska State Statute to reference the federally-mandated exception for absent uniformed services voters and overseas voters being sent their ballots no later than 45 days before election day.

- Amend Alaska State Statute to clarify that those voters who are traveling or working outside of the United States at the time of the election would receive special absentee ballots.

- Amend Alaska State Statute to move up the date of the primary election to the second Tuesday in August of every even-numbered year, rather than the fourth Tuesday in August of every even-numbered year.

- Amend Alaska State Statute to change the deadline for candidate withdrawal from the primary election to "before June 22 of the election year" rather than "at least 48 days before the date of the primary election."

- Amend Alaska State Statute to remove the prohibition that votes for a write-in candidate not be counted unless that candidate has filed a letter of intent with the director.

- Amend Alaska State Statute to change the deadline for filing a letter of intent to run as a write-in candidate to 21 days before the General Election, so the division can more effectively provide assistance to voters.

- Amend Alaska State Statute on filling candidate vacancies by party petition to extend the deadline to before September 3 of the election year, rather than 48 days or more before the general election.

Recommended changes in election procedure:

- Provide multiple notices to the political parties to ensure the parties are aware of their ability to nominate election workers. After the nomination deadline, the division will, if necessary, request assistance from the political parties in locating workers to keep the election board balanced.

- As more Alaskans are taking advantage of early and absentee voting, the division will examine how and whether it can report all results by precinct in future modifications of ballot counting and reporting software.

- Improve training and written instructions to election workers about the need to mark the type of identification presented by the voter on the polling place register.

- Add instructions to the voted ballot envelopes to remind workers to sign across the seal and improve election worker training relating to ballot security.

- To improve election management, the division will replace the voter registration and election management database system with a more technologically advanced system.

- The division will also implement additional security measures of using tamper-proof seals on archive boxes and numbering envelopes sent out prior to transporting ballots to a counting center.

- To improve how unvoted ballots are handled and accounted for, the division will make changes to the ballot statement to specifically include the number of ballots received, used and destroyed. The division will also report the return of the ballot stubs from unvoted ballots that would prevent any use of ballots for fraudulent activity.

- To address concerns that more write-in votes were counted than initially reported on the election results. In the future, the division will ensure that blank ballots that get challenged but that are not counted are not included in the overall results.

- The division will work to research systems to provide "real-time" or electronic updates identifying which voters have voted.

- The division will also post information to the website that indicates the date when absentee ballots are being mailed, filing deadlines, withdrawal deadlines, state review board dates.

- To ensure ineligible felons do not vote, the division will complete the data match between the Department of Corrections and the state voter registration file immediately prior to each election.

- In the case of an election which may be contested the division will re-brief election officials on the need to maintain objectivity and non-partisanship.

- To make it easier for military members to vote, we recommend changing the date of the primary to make sure ballots for a general election can be in the mail in time for service members overseas, allowing other electronic forms of transmissions of ballots back to Alaska (the law currently limits electronic transmission to faxes). The division suggests the under the new redistricting plan, the precinct boundaries be changed so that only installation boundaries are included in the precinct. When precincts are wholly contained within the installation, the division can once again work with the military to establish polling places on the bases. This report recommends this change to the Redistricting Board.

Recommendations to other parties:

- Suggest that the Redistricting Board redraw precinct boundaries specific to military installation in order to move the polling places back to the bases.

- The report discusses a proposal Alaska is considering to further exchange information on Alaska state voters with several data sources in other states in a bonded, confidential manner, in order to identify the names of voters who may be registered in more than one state.

Recommendations for third party review:

- Review of division's audit procedures and hand count verification of election results
- Audit to ensure non-U.S. citizens are not voting
- Audit to ensure that felons are not voting.
- Explore system or methods that can provide for real-time voter history.

2010 General Election Review
Office of Lieutenant Governor Mead Treadwell

The 2010 General Election in Alaska was historic. Only on two other occasions has a significant statewide write-in campaign been conducted. The election revealed sections of election law and procedures that were yet untested, and many Alaskans became more aware of election procedures. Alaska's write-in process was widely publicized, and the state was pleased to see that process upheld by the state and federal courts.

After Governor Sean Parnell and I signed the final paperwork to certify the 2010 General Election, I announced we would conduct an election review to examine lessons learned in the way the election was conducted. A review could also help fully explain the election process to Alaskans. This review, by the Office of the Lieutenant Governor, the Division of Elections and the Department of Law, includes an analysis of election laws and procedures as well as feedback from stakeholders, political parties, and most importantly, Alaska's voters. The resulting report responds to observations and concerns made by Alaskans, and offers a recommendation for change or retraction of current procedures, Alaska State Statute, and/or regulation for each issue.

A key recommendation as a result of this review is intended to make it easier for Alaskans serving in the military to vote. Those recommendations include changing the date of the primary to ensure ballots for a general election can be in the mail in time for service members overseas; allowing other electronic forms of transmissions of ballots back to Alaska (the law currently limits electronic transmission to faxes); and working with the Redistricting Board and the Department of Defense to facilitate reopening of polling places on Alaska's military bases.

Other key recommendations include changes to state law to clarify procedures for counting write-in ballots and making the declaration of candidacy for a write-in candidate voluntary. Perhaps the single most important finding in the review is that no change in procedure or state law recommended would have changed the outcome of the 2010 General Election.

To maintain objectivity in the examination of certain questions aimed at the Division of Elections, the report recommends third party review on specific issues.

Our heartfelt thanks goes out to those who worked so tirelessly on the 2010 General Election, including former Lieutenant Governor Craig Campbell, division personnel, attorneys from the Department of Law, candidates, and especially the volunteers who so selflessly gave their time and energy to bring the election to a conclusion. And thanks are due to Alaskans for taking their time to submit comments, to stakeholders for meeting with the Lieutenant Governor, and to the Division of Elections, with special thanks to Director Gail Fenumiai, and Department of Law for their assistance in this review.

Mead Treadwell
Lieutenant Governor

I. Overview of Processes

I. (A) Polling Place Procedures and Election Worker Training

1. Election Worker Recruitment

Election worker recruitment is one of the more time consuming tasks in conducting a successful election. Recruitment begins around March of an election year and continues, in some cases, right up to election day. As part of the recruitment process, the division notifies the political parties that they are eligible to nominate election workers as outlined in AS 15.10.120. By law, political party nominations are due by April 15th of the election year.

Depending on the size of the precinct, each polling place has approximately three to six election workers. In an effort to maintain consistency within the polling places, the division requests workers to work both the primary and general elections and to work the entire time the polls are open, 13 hours. Whenever possible, the division attempts to find workers who are registered voters of the precinct. If the division is unable to locate voters within the precinct who are willing to serve, the division will recruit any qualified voter.

The first worker recruited for each precinct is the chairperson. The chairperson is then requested to assist the division in locating the remaining workers for the precinct. Public comments were received suggesting that allowing the chairperson to recruit other board members is conducive to partisanship or fraud. Others suggest that there should always be a representative from each political party on the election board. The division has not found any evidence of fraud on the part of election workers. Having the chairperson assist with the recruitment of other election board workers helps to create a positive experience for the workers which in turn allows for a positive voting experience for the public. It also allows a wider pool of potential workers to be contacted. The division has also found that when workers enjoy those whom they are working with, they are more likely to continue to be election workers from one election to another, which creates a more experienced election worker pool.

When recruiting the election board workers, the division and the chairperson attempt to ensure the election board is politically balanced and that there is political party representation on the election board. Although the division sends political parties a notice of the deadline for them to nominate election board members, comments were received that the division does not provide sufficient notice. For future elections, the division will provide multiple notices to the political parties to ensure the parties are aware of their ability to nominate workers. After the nomination deadline, the division will, if necessary, request assistance from political parties in locating workers to keep the election board balanced.

The chairperson is paid $10 per hour for their time at the polls and the other election workers are paid $9.50 per hour. Workers are compensated for their time spent in training if the trainee works in the election. The division has received comments from

workers that it would be easier to find election workers if the pay was increased.

The last increase for election workers of $2/hour was in 2004.

Any increase to election worker pay would require a budget increase to the division in an election year. There is no provision for an increase in FY12 budget as any change for the 2012 Primary or General Elections would be appropriated in the 2013 fiscal year beginning July 1, 2012.

The division has approximately 2500 precinct election workers (those that work at polling places on election day). They work 15 hours per election.

$9.50x15=$142.50

If they were to get a raise to $15/hour:

$15x15 = $225

For a difference of $82.50 per election worker per election.

$82.50x2500x2 elections = **$412,500** budget increment

An increase to $12/hour would result in a budget increment of **$187,500.**

This report makes no recommendation on salary increases; however, recommendations will be made in time for the Governor's 2013 fiscal year budget proposal.

2. Election Worker Training

The division's four regional offices are responsible for training precinct election board workers in their respective regions. In-person training is conducted prior to each primary election for the election board workers across the state. It is the division's goal to train workers as close to the election as possible. However, with the large number of rural precincts, some regions have to begin their worker training in early June and continue until early August.

Concerns and comments were received about the division not using standardized training materials throughout the state. Although there are differences between urban and rural, hand-count and optical scan count precincts, the division does in fact use a standardized set of training materials and handbooks to train all precinct election workers depending on the type of precinct they work in (optical scan or hand-count). There is a standardized set of instructions and handbooks for all optical scan precincts and there is a standardized set of instructions and handbooks for all hand-count precincts. In addition, there is a standardized set of instructions and materials developed for the touch screen equipment that is provided to all precincts.

In-person training sessions are approximately four to six hours in length and are broken

into two modules: election procedures and equipment procedures. The election procedures module covers areas such as opening the polls, providing voter assistance, disability awareness, language assistance, processing voters, issuing ballots, questioned voting, special needs voting, closing the polls, completing the ballot statement and returning election materials.

For precincts that hand-count their ballots, this module also includes instructions on how to count ballots and report election results. The equipment module covers functions necessary to set up the equipment (optical scan and touch screen) and prepare it for voting. The training also covers the process for how to maintain security of the equipment, functionality and operation of the equipment, and the process for transmitting results. The equipment procedures module gives workers hands-on experience and practice setting-up, voting, printing election results and disassembling the equipment.

The division conducts training for workers in rural areas of the state in several "hub" cities. Election workers from selected rural precincts travel to a larger, more "central" community to receive training as a group. Since Alaska has a very large number of precincts that are not on a road system, utilizing hub training enables the division to train rural workers closer to election day and reduces the amount of travel time needed by division staff. Urban-based training is generally conducted closer to election day and is conducted with workers from multiple election boards present.

Although in-person training is conducted before the primary election, the division offices in Anchorage, Fairbanks, Juneau, Mat-Su and Nome review election procedures with precinct chairpersons when they pick up their materials from the regional offices. A written review is sent to all other precincts.

The division faces many challenges with information retention between the time of the training and the election, especially in rural areas of the state where training is usually conducted more than a month before the primary. In addition, workers quit and are replaced after the training takes place. The division's standardized set of instructions and handbooks is critical to the workers' ability to perform their duties correctly. In 2010 the division created a training video to send with election supplies that covers the same topics as the in-person training sessions.

Although the division provides a comprehensive training program for workers and uses a standardized set of instructions and training materials across the state, there will inevitably be times when election board workers simply forget to perform an outlined process or procedure. When the division becomes aware of those situations, its managers will take steps to address the issue.

3. Polling Place Procedures

On election day, election board workers have a standardized set of instructions to follow when opening the polls, processing voters, and closing the polls. When the division receives comments, concerns or complaints about problems in a polling place on election day, the division makes contact with the workers to address or correct those issues.

a) **Voter Identification**

Under AS 15.15.225, election workers are required to request identification from voters. However, workers can waive the identification requirement if the voter is personally known, unless the words "Must Show ID" appear in the signature box on the precinct register. Workers are also instructed to check the box on the register indicating the type of identification presented. If a voter does not have identification and does not meet the waiver requirements, the voter must vote a questioned ballot.

After the 2010 General Election, there were concerns that election workers allowed voters to vote without requiring identification because boxes were not checked to indicate the type of identification shown.

The division contacted 24 precincts where the "Identification Presented" box was not checked either for 100% of the voters or for some portion of the voters, to determine if the workers allowed voters to vote without requiring identification. Each precinct confirmed that they did require voters to show identification unless the voter was personally known. If the voter didn't have ID, they had the voter vote a questioned ballot. When asked why they did not check the "Identification Presented" box, the workers responded with comments such as:

i. We simply forgot.
ii. We were unaware this was necessary.
iii. We were too busy and must have overlooked the box.
iv. We were asked to highlight signatures and this caused extra time and work, and we must have just gotten too busy with the extra requirement.
v. We don't have to mark the box for municipal elections so we didn't think we needed to for state elections.

In contacting the precincts the division found no indication of misconduct on the part of the workers and concludes that blank "Identification Presented" boxes were simply an oversight. The division is committed to improved training and written instructions about the need to mark on the register the type of identification presented.

b) **Ballot Security**

When the polls close, election workers seal the voted ballots in special tyvek envelopes. After the tyvek envelope is sealed, an opened envelope becomes evident because the seal is broken. As an added security measure, after sealing the envelope(s), workers are instructed to sign across the seal before returning the ballots to the Division of Elections.

After the 2010 General Election, the division received voted ballot envelopes that were sealed but that did not have election worker signatures across the seal. After working a 13+ hour day, workers are ready to go home and sometimes overlook signing across the seal.

In no case had the initial seal on the envelopes been broken, but the division recognizes the absence of signatures caused the perception of compromised ballot security during the tabulation of the write-in votes.

Public comments were received related to the improvement of ballot security. Although ballots are sealed in tyvek envelopes, improvements are needed to ensure that workers sign across the seal. The division takes ballot security seriously, and will add instructions to the voted ballot envelopes to remind workers to sign across the seal. The division will also make improvements to election worker training relating to ballot security.

c) **Unvoted Ballots**

When the polls close, election workers in precincts outside of Anchorage, Fairbanks, Juneau, Mat-Su and Nome are instructed to destroy their unvoted ballots. Precincts in Anchorage, Fairbanks, Juneau, Mat-Su and Nome bring their unvoted ballots back to the division's regional offices to be destroyed.

Public comments were received relating to the handling of unvoted ballots. One suggestion was that election workers should be required to sign documentation indicating the ballots were destroyed. The division instructs the election workers to complete a ballot statement indicating how many ballots were used after the polls close. This statement, along with the signatures in the precinct registers, allows the division to account for all ballots and to ensure that the election results do not include extra ballots. In an effort to improve how unvoted ballots are handled and accounted for, the division will make changes to the ballot statement to specifically include the number of ballots received, used and destroyed. The division will also investigate whether it is possible logistically for the return of ballot stubs from unvoted ballots to further prevent any use of ballots for fraudulent activity.

I. (B) Impacts on Process Relating to Distribution of Write-In List

There have been two major write-in campaigns for a statewide election in the past two decades. In 1998, Robin Taylor ran as a write-in candidate for governor. In 2010, Lisa Murkowski ran as a write-in candidate for United States Senate. The difference between the two elections was that in 1998 Alaska Statutes did not require write-in candidates to file any form of declaration with the Division of Elections. After the 1998 election, the statutes were changed to require write-in candidates to file a letter of intent with the division at least five days prior to the election.

The division consulted with the Department of Law to determine what assistance by an election worker was allowable to those voting for a write-in candidate. The division and Department of Law concluded that a list of declared write-in candidates should be distributed to election workers in order to ensure that workers provide consistent, standardized assistance to voters on write-in questions. The division also believed that providing a list would help minimize disruption in the polling place that might result from conversations between poll workers and voters regarding write-in candidates. Election workers were instructed not to post the list, but to have it available for reference upon request of the voter.

Since providing a list of write-in candidates to the election workers was a new procedure, the division submitted the change in practice to the United States Department of Justice (DOJ) for preclearance as required by Section 5 of the Voting Rights Act. DOJ precleared the change prior to the distribution of the list.

1. Impacts on Public Perception

The implementation of a write-in list triggered a lawsuit filed against the division, and the Alaska Supreme Court ruled in favor of the division's use of the list. As a protest to the Supreme Court's order allowing the write-in list, a radio talk-show host went on air and encouraged listeners to file paperwork with the division to become declared write-in candidates so that poll workers would have a difficult time finding Lisa Murkowski's name on the list.

Prior to the radio broadcast, there were only a few declared write-in candidates for the U.S. Senate race. The broadcast resulted in 168 write-in candidates for U.S. Senate.

Several public comments were received both prior to and after the election indicating that the division should not have distributed a write-in list. Some members of the public also made comments to the division that they believed the division provided the list as a way to help one candidate over another. The division implemented the list as a way to ensure that effective voter assistance could be provided, and this decision was affirmed by the Alaska Supreme Court.

The requirement for a write-in candidate to file a letter of intent restricts a time-honored tradition voters have in most states. The right to cast a write-in vote exists as a "release valve" in the event a voter is not happy with the choices available on the ballot. The Division of Election's job is to empower voters. Therefore, the recommendation is to change Alaska State Statute to make it voluntary for write-in candidates to file a letter of intent. At the same time, we recommend making the voluntary write-in letter of intent dealing 21 days prior to the general election day.

I. (C) Processes and Procedures for Counting Write-In Votes

1. Internal Preparation and Procedures

a) Establish date/time for counting of write-in votes

6 AAC 25.085 establishes the criteria used to determine when the counting of individual write-in votes must be performed. This regulation further outlines that the director will establish the place and date for counting write-in votes.

For 2010, the director initially established that if the number of write-in votes cast in the election was sufficient to trigger counting, the counting would take place in Juneau beginning the 16th day following the election. The date was selected based on the fact that the last count of absentee ballots is performed on the 15th day following the election, and the division might not know if the threshold requirement for conducting the count of individual write-in votes would be met until all ballots were counted. It was initially reported to candidates and the public that the date would be the 16th day following the election.

After results were posted on election night, it was clear that the division would be required to separate and count the individual write-in votes. Lieutenant Governor Campbell indicated it would be in the best interest of the state and public if the write-in votes were individually counted sooner than initially planned. It was determined that the division would begin counting the write-in votes on November 10th, and candidates were notified. The Department of Law advised that the lieutenant governor's decision was legal and appropriate, and the court backed this up.

b) Establish location and secure workers

AS 15.15.370 requires all ballots to be sent to the director. The division also relied on 6 AAC 25.200, which requires all recounts to be conducted in Juneau, because a recount is a similar procedure to counting write-in votes. Since all ballots are sent to Juneau following an election, the separation and counting of write-in votes was conducted in Juneau.

The division secured a counting facility that could accommodate 15 teams of counters consisting of two people using two 3' x 5' tables, press, public viewing and observers. In addition, a vendor was secured to transport the tables and chairs necessary for the workers.

The location established allowed for a secure counting area and ballot storage area with limited access. There was also a designated area set up for press and a designated area for the public to observe the counting process without being in the immediate counting area.

c) **Recruit and train workers**

It was determined that 15 teams of two workers would be used to perform the separation of the write-in ballots. In addition, alternate workers were identified in the event that an appointed worker was unavailable during counting times.

The division required all workers to attend a pre-counting training session. The training covered the processes and procedures that would be used when separating ballots.

Each day of the counting, the workers had to sign in and out and were given badges to gain access to the immediate counting area. The workers' political party affiliation was taken into consideration when pairing the teams so that there would not be a team consisting of two workers of the same party affiliation. Each team was assigned a table number, and the division maintained a list of table assignments.

d) **Ballot security**

Counted ballots are sealed in tyvek envelopes by the precinct election board or counting boards before being transported to Juneau for storage and archiving. The outside of the ballot envelopes indicate the district/precinct of the ballots. Election workers are instructed to sign across the seal on each ballot envelope.

When ballots arrived in Juneau, division staff recorded the ballots received, and indicated the number of ballot envelopes for each district/precinct. After the ballots are recorded, the sealed envelopes are placed in archive boxes by district and secured in an alarmed ballot room.

The division contacted several security contractors and ultimately, secured the services of the only company that had transportation available and could meet the division's request. The security contractor was hired to transport the sealed ballot envelopes contained within archive boxes to the counting center. Each time the ballots were transported, the security contractor and the division recorded each ballot envelope on a transport log. The log was completed and signed when the ballot envelopes left the alarmed ballot room, when they arrived at the counting center, when they left the counting center, and again when they were received back in the ballot room.

While in the counting center, the ballots were stored in an open, cordoned-off area that allowed access only by division personnel and the security contractor. Before taking ballots from this area to a counting table, they were checked-out and recorded on a table assignment list, and they were checked back in upon their return.

Comments were received from the public regarding the transportation of ballots to/from the counting center in archive boxes. Comments were also received about division personnel and the security contractor having sole access to the ballots. Since the ballots in the archive boxes are sealed inside ballot envelopes, they are secure during transportation. And to further ensure security, the division already numbers the envelopes. The division will implement additional security measures of using tamper-proof seals on archive boxes sent out prior to transporting ballots to a counting center.

e) **Recording write-in vote results**

In order to record the write-in results for the large number of declared write-in candidates, the division created an election database using the GEMS ballot tabulation system software. The write-in database included the names of each write-in candidate. The division believed there would be a large number of challenged ballots, so it also decided to create a category in the database to record the number of "challenged counted" and "challenged – not counted" ballots. The "challenged – not counted" category was created because the division felt there would be ballots that could not be counted for a write-in candidate but that would be challenged. In addition, the database included a category to record the names of write-ins for candidates who did not file a letter of intent. The division also included in the database write-in votes for names appearing on the ballot, because it is not uncommon for a voter to write in the name of a candidate appearing on the ballot.

Many ballots were discovered during the write-in count process in which the voter failed to mark the write-in oval, but wrote in the name of candidate Lisa Murkowski. When sorting and counting the individual write-in votes, the division followed Alaska State Statute, which indicates that if the oval was not marked, the write-in vote cannot be counted. These are considered blank ballots and were not included in the initial write-in vote totals.

Prior to separating and counting the individual write-in votes, the election results did not include write-in ballots in which the oval was unmarked though a name was written in. These are considered blank votes for that race. After challenges by the Murkowski campaign, these ballots were recorded with the "challenged – not counted" ballots, because there was no category specifically for recording write-in ballots with unmarked ovals. This category, however, included other ballots where the write-in oval was marked but were recorded as "challenged – not counted" for other reasons.

Since the write-in results for the US Senate Race included these blank ballots which were challenged by the Murkowski campaign, the results appeared to have more write-in votes than originally reported. However, the additional ballots were never valid votes, but were later recorded with other uncounted ballots when the Murkowski campaign challenged them.

In the future, the division will ensure that blank ballots that get challenged but that are not counted are not included in the overall results.

f) Access to counting area

The division established a sign-in/sign-out process to control access into the immediate counting area. In order to gain access to the counting area, each counting worker and observer had to sign-in and each was given a badge.

The division allowed one observer from each campaign to be present at each table in the counting area. In addition, each campaign was allowed to have a lead observer present in the counting area.

In addition to the workers and observers, the division required press members to sign in and wear a press badge. Press members had their own area with full viewing access of the counting. As requested, the division allowed a limited number of press members in the immediate counting area for short periods of time to take pictures or film footage. When press members were in the immediate counting area, they were accompanied by division personnel.

Division personnel and Department of Law personnel also wore badges.

Although the public was not allowed in the immediate counting area, the division did establish an area for the public that allowed full viewing access.

Comments were received that the division politicized the write-in count process by roping off areas after challenges to ballots began. The division provided equal access to the counting area for both the Murkowski and Miller campaigns. Access was established on the very first day and remained consistent throughout the counting process.

Access to the cordoned-off area where the ballots were being held, which was visible to all parties, was limited to division personnel, Department of Law personnel and the security contractor. At no time did observers for either candidate have access to this area.

2. Counting Individual Write-In Votes – U.S. Senate Race

When separating ballots to count the individual write-in votes, the ballots were first sorted. After the initial sort, the director, with the assistance of the Department of Law, made a determination on voter intent. Once voter intent was determined, the ballots were counted and the individual write-in results recorded.

Below is an outline of the process:

a) Initial Ballot Sort

There were five boxes used to sort ballots. The boxes were used to initially sort the ballots as follows:

i. All ballots where the oval is marked next to a candidate's name that is printed

on the ballot (those other than the "Write-In" category) were placed in box #1.

ii. All ballots where the U.S. Senate Race is left blank (no oval marked) or more than one oval is marked were placed in box #2.

iii. All ballots where the oval is marked for the "Write-In" category and the name is written as "Lisa Murkowski" or "Murkowski" and spelled correctly that were not challenged were placed in box #3.

iv. All ballots where the oval is marked for the "Write-In" category and the name written in is "Lisa," "Lisa M" or other variations that demonstrated the voter is casting a ballot for Lisa Murkowski were placed in box #4. This box was also used for workers to place any ballot voted for Lisa Murkowski that an observer challenged so that the director could make a determination on voter intent.

v. All ballots where the oval is marked for "Write-In" category and the name written in is for a candidate other than Lisa Murkowski or variation of Lisa Murkowski were placed in box #5.

During the first day of sorting, some teams sorted the ballots into the five boxes so that the candidate names were facing the sorting team, and some sorted so that the candidate names were facing the observers. The division received comments from the observers that they would like all sorting teams to sort the ballots so that the candidate names printed on the ballot faced the observers. The division implemented this change on the second day of sorting. Although comments were received that ballots were sorted upside down, this only happened on the first day and was corrected by the division at the request of observers and had no effect on the result of the election.

b) Director Determination

i. Each ballot in box #2 (blank and overvoted ballots) was reviewed to verify the ballot is truly blank or overvoted.

ii. Each ballot in box #4 was reviewed to determine voter intent. When reviewing these ballots, they were sorted into three categories as follows:

1) Determination made to count as vote for write-in candidate Lisa Murkowski and determination is not challenged. (These ballots were placed in box #3 for counting.)

2) Determination made to count as vote for write-in candidate Lisa Murkowski and determination is challenged. These ballots were segregated and placed into an envelope labeled "Challenged – Counted for Murkowski." The total number of votes from these ballots was recorded on the results sheet as votes for "Murkowski – Counted Challenged."

3) Determination made to not count the vote for write-in candidate Lisa Murkowski and determination is challenged. These ballots were segregated and placed into an envelope labeled "Challenged – Not Counted for Murkowski." The total number of votes from these ballots were added to the results sheet as "Murkowski – Not Counted Challenged."

c) Recording Results

i. The ballots from box #3 (votes for Murkowski) were hand counted and the total number of votes was recorded on the results sheet for "Lisa Murkowski."
ii. The number of ballots in the "Challenged – Counted for Murkowski" envelope was hand-counted and recorded on the results sheet line "Lisa Murkowski – Counted Challenged." After counting, these ballots were returned to the envelope.
iii. The number of ballots in the "Challenged – Not Counted for Murkowski" envelope was hand-counted and recorded on the results sheet line for "Murkowski – Not Counted Challenged. After counting, these ballots were returned to the envelope.
iv. For the ballots in box #5 (write-in votes for candidates other than Murkowski), the workers sorted the by name. Once the ballots were sorted, the workers counted and recorded the individual results for candidates appearing on the write-in candidate list. If the name written in did not appear on the certified write-in candidate list, workers recorded the votes on the line for "Other Write-In."
v. After the workers recorded the write-in votes on their results sheet, division personnel compared the total number of individual write-in votes to the write-in category on the initial statement of votes cast. This was done to make sure counting workers did not accidentally place write-in votes in box #1.
vi. Once the total number of write-in votes was verified, the workers sealed the ballots in the original voted ballot envelope(s) and the results sheet used to record the individual write-in votes was given to division personnel to enter into the GEMS database.

3. Timeline

The division began the individual counting of write-in votes on Wednesday, November 10th. Initially, the division thought that it would take three to four days to conduct the count. However, due to the large volume of challenged ballots, the division did not complete the counting of write-in votes until November 17th. This fact alone confirmed Lieutenant Governor Campbell's decision to begin the count earlier.

Each day, the counting began at 9am and went to approximately 4-5pm. On Sunday, November 14th, the division did not begin the counting until noon.

On November 19th, the division counted the write-in votes from special advance and overseas ballots. The initial count of these ballots took place in the regional offices on the 15th day following the election, and the ballots were shipped to Juneau. The division notified the campaigns and press that the write-in separation from these ballots would take place in the Division of Elections director's office on November 19th.

4. Cost

The total cost to individually count the write-in votes was $60,440.

I. (D) Successes

Alaska faces logistical challenges to ensure that all 438 precinct polling places across the state are open and staffed, and receive their ballots, supplies and equipment. Accomplishing this is a success in its own. There were other notable successes relating to the 2010 General Election:

1. Litigation

During the 2010 General Election, there were several lawsuits filed against the division in both state and federal courts.

The main issue in the litigation was related to the division's decision to provide a list of write-in candidates to the poll workers and the division's process to count write-in votes, including determining voter intent.

The state and federal courts ruling in the division's favor was the most notable success of the 2010 General Election.

2. Implementation of the MOVE Act

Under the new requirements of the MOVE Act, the division was required to mail ballots to military and overseas voters at least 45 days prior to the general election and late candidate withdrawal deadline. Due to the short time frame between the primary and general elections, the division initially applied for a waiver to this requirement. The division was notified the waiver was denied and the division was required to develop a process that would allow ballots to be mailed 45 days before the general election.

The statutory candidate withdrawal deadline of 48 days prior to the general election made it impossible to have official ballots printed in time to meet the MOVE Act 45-day ballot mailing requirement. The division developed a process to produce an in-house paper ballot which was mailed to over 8,000 UOCAVA voters by the deadline.

To count the ballots using the division's optical scanners, the absentee ballot review boards had to produce a facsimile of the ballot using an official ballot printed on ballot stock. Although this caused extra work for the review boards, the division was able to meet the statutory deadline for reviewing and counting ballots.

3. Election Worker Training Video

In an effort to supplement in-person training, the division created an election worker training video that covered the same components as the in-person training sessions. The video provided workers with an opportunity to be trained even if they were unable to attend the in-person training. The division received positive feedback from election workers who found the video valuable.

4. Federal Observers in Bethel

The division was notified approximately one week before the general election that the Department of Justice would be sending federal observers to Bethel. In order to prepare for the observers, the division worked with Lori Strickler, Bethel City Clerk, to set up a training session for the poll workers the weekend before the election to go over election procedures and to inform the workers about the observers. The division's Yup'ik Language Assistance Coordinator was on-site in Bethel for election day.

Although it was intimidating for poll workers to have federal observers watching them, the division and poll workers were prepared and successfully conducted the election in Bethel. There is, however, no after action report available from the Department of Justice.

5. Counting Write-In Votes

In addition to the normal post-election processes, in 2010 the division had to prepare for and count the individual write-in votes for United States Senate. The counting was high-profile, with both national news media and campaign observers present.

The division created a process to separate and count write-in votes from 258,746 ballots cast in the 2010 General Election. Throughout the process, the division was able to maintain security and organization of a very large volume of ballots and election materials.

The division updated the press, campaigns and the public each day with ballot counts and results.

I. (E) Issues for Improvement

1. Implementation of MOVE Act Requirements

The division was successfully able to meet the 45-day deadline to mail absentee ballots to military and overseas voters by preparing a paper copy of the ballot. Although this allowed the division to meet the requirement, it impacted the amount of time to count absentee ballots and resulted in a large number of facsimile ballots. Statutory changes should be pursued that will allow for the official ballot, rather than a facsimile, to be sent by the 45-day deadline.

Currently, absentee ballots must be mailed or faxed to voters. The division received numerous comments from military and overseas voters that they do not have ready access to fax machines and requested their ballots be sent via email. Statutory changes should be pursued to allow blank ballots to be transmitted via email.

It is recommended that legislation be introduced to change the date of the primary election; change the candidate withdrawal deadlines for the primary and general elections and change the party replacement deadlines for the primary and general elections.

2. Voter Registration Database

The division's voter registration and election management database was developed in 1985 and is a mainframe-based system. Because the technology is antiquated, there are a limited number of programmers available that have experience in this programming language. In addition, it is costly to maintain at an annual fee of over $100,000 per year. The division needs to replace this system with a more technologically advanced, PC-based system.

3. Election Worker Pay

Each election, the division struggles to recruit poll workers. These workers are required to work a 13+ hour day with a great deal of responsibility. A pay increase could result in more people willing to serve as poll workers and result in more participation from political parties.

This report makes no appropriation recommendations.

4. Hand Counting Ballots

There are 133 precincts in Alaska that hand count their ballots after the polls close and call the regional offices with their election results. Once received, the regional offices enter the results into the regional tabulation server which is then uploaded to the host server in Juneau. If the election board calls in the wrong number of voters, or wrong results, the regional offices enter incorrect information which then has to be corrected by the State Ballot Counting Review Board. Although improvements have been made to training methods, the division will need to continue to improve materials to address hand counting of ballots.

5. Voter History

Prior to opening and counting absentee and questioned ballots, the division conducts a duplicate analysis to verify that the voter did not vote more than once. This duplicate analysis cannot be performed until all voter history is completed from the precinct registers used in the polling places. Until the duplicate analysis is complete, absentee ballots cannot be opened and counted. This causes a delay in opening and counting the absentee ballots.

To enhance the voter history process, the division will research the feasibility of implementing the use of electronic poll books. Electronic poll books could potentially expedite the counting of absentee and questioned ballots by more quickly recording voter history and conducting duplicate voter analysis.

An online real-time voter history system would have several advantages:

a) It would expedite the counting of absentee and questioned ballots
b) It would identify individuals attempting to vote more than once in any given election, avoiding potential fraud
c) It could allow observers, candidates and parties to focus their get-out-the-vote efforts more effectively, and perhaps increase turnout altogether.

I. (F) Statistics and Analysis

There are 438 precincts in Alaska. In order to conduct an election, the Division of Elections ensures each precinct has a polling location, workers to run the polling place and that each location has the ballots, supplies and equipment needed for the election.

There are 305 precinct polling places that use an optical scan machine to count ballots. There are 133 precinct polling places, located in rural areas of the state, that hand-count their ballots when the polls close. During the primary and general elections, there is also a touch screen voting unit in each precinct polling place that is intended for use by voters who have visual impairments, disabilities or have difficulty reading.

1. How many people voted

260,976 voters voted in the 2010 General Election, of which, 258,746 ballots were counted and 2,230 ballots were rejected.

Following is a breakdown of the ballots cast:

192,940 cast ballots on Election Day and counted at the polls
11,698 counted questioned ballots
1,297 rejected questioned ballots
40,843 counted absentee ballots
933 rejected absentee ballots
13,265 counted early ballots

There were 494,876 registered voters qualified to vote in the election. Overall percentage turnout based on the counted ballots was 52.29%. The percentage turnout in the 2010 election is slightly higher than in previous gubernatorial election years.

2. How many people cast write-in votes

Out of the 258,746 cast ballots, there were 102,234 votes cast for write-in for the U.S. Senate race.

Although there were write-in votes for each race on the ballot, only the write-in votes cast in the U.S. Senate race met the required threshold to count the individual write-in votes.

3. Cost and length of time to count write-in votes

It cost the division $60,440 to conduct the counting of the write-in votes for the U.S. Senate race.

The counting of the write-in votes started on November 10th and concluded on November 17th with a small number of ballots being counted on November 19th.

4. Reporting absentee and early vote results by precinct

Comments were received indicating that results from absentee and early voting should be reported by precinct. Unlike precinct polling place ballots, absentee and early ballots are issued at the house district level, not at the precinct level. Alaska State Statute 15.20.201 requires the district absentee ballot counting board to review and count absentee ballots. The division's existing voter registration and election management database is programmed and designed to track absentee and early ballots by house district.

Having both systems designed to manage absentee and early ballots by house district allows for the public and candidates to get a list of all absentee and early voters and to see election results by house district. This also allows the division to verify that the number of ballots accepted for counting matches the number of actual ballots reported in the election results which is critical to the ballot accountability process.

As more Alaskans are taking advantage of early and absentee voting, the recommendation is for the division to examine how and whether it can report all results by precinct in future modifications of ballot counting and reporting software.

5. Providing information on absentee voters

Comments were received that it is difficult to get information from the division about voters who requested absentee ballots and that the division mailed ballots to voters earlier than the announced date.

The division's absentee office produces an updated absentee voter report following each mailing. If an organization has purchased the initial absentee list, their name is kept and they are automatically sent subsequent lists. The division's absentee office consistently provides lists to candidates and parties.

The division believes that mailing absentee ballots to voters as soon as they are available is critical to the voter's ability to receive a ballot in time to vote. Once ballots are sent, the updated absentee voter report provided to the candidate and parties includes the date the ballot was mailed. In an effort to ensure this information is more readily available, the division will post information to the website that indicates the date when ballots are being mailed, or mesh this system with a planned online real-time voter history system.

2010 Election Review
II. Answering Alaskans' Questions

II. (A) Voter Intent

Question: Should voter intent be included as part of the rules for counting write-in votes?

This report recommends yes.

There is legislation pending in the 2011 legislative session that considers this question. Senate Bill 31 has passed the State Senate and is awaiting hearings in the State House. This legislation codifies the decision of the Alaska Supreme Court that voter intent must be considered when counting ballots.

There were public comments received that voter intent should not be included in determining whether or not a ballot should be counted. The Alaska Supreme Court has historically and repeatedly encouraged the division to implement and honor voter intent in counting ballots. This was again the case with their order in December 2010.

II. (B) Letter of Intent for Write-In Candidacy

Question: Should there be continued requirements for individuals to file their intent to be a write-in candidate and if so, what is realistic time requirement for filing such intention?

Today, Alaska State Statute requires a write-in candidate to file a letter of intent to run for public office within five days of a general election. The requirement is relatively new in Alaska law and had never been tested before the 2010 General Election, when the list of write-in candidates itself and its use in voting locations was challenged in State courts.

As a result of this review, it is recommended that the requirement for filing a write-in letter of intent be voluntary, not mandatory. This would maintain the voters' freedom to use the write-in process to vote for whomever they choose. However, if a candidate desires to file a write-in letter of intent, the division could more effectively provide assistance to voters if the requirement is changed so that the letter of intent must be received by the division no later than 21 days before the general election. If appropriate thresholds are met to require the individual counting of write-in votes, nothing should preclude a candidate who has not filed a write-in letter of intent to have his or her votes counted.

With the understanding that the circumstance for a write-in candidate to run and not file a letter of intent is rare, yet may be necessary to ensure each party has a candidate in the election, the division will continue to encourage write-in candidates to file a letter of intent for election for the following reasons:

1. Filing a letter of intent verifies that the individual running for office meets the constitutional and state requirements for the office.

2. The letter of intent provides the division with the framework for how the candidate's name should be written.

3. Without knowing in advance, the names of write-in candidates, voters who wish to vote for a write-in candidate could be disenfranchised if they needed assistance in voting for a candidate.

4. The candidate filing requirement is helpful for the division's preparation of the write-in candidate list for use in the polling places on Election Day. This list helps with voter assistance, which is required by both Alaska Statute and by federal law.

5. The write-in candidate list was precleared by the U.S. Department of Justice (DOJ) last year. To discontinue using the list would require preclearance.

6. Registration also allows the state to enforce financial disclosure laws and electioneering laws against all candidates equally.

II. (C) Felons Voting

Question: What additional precautions, if any, are necessary to prevent felons from voting?

The division has a process in place to remove voters that have been convicted of a felony involving moral turpitude for the voter rolls.

The division receives a list from the Department of Corrections and processes the names on the list. Prior to removing a voter, the division must verify the conviction is for a felony involving moral turpitude. This process is conducted, at minimum, on a bi-weekly basis.

The division seeks the assistance of the Department of Law to determine if a crime meets the legal definition of "moral turpitude" if the crime listed is not found in AS 15.80.010(9).

There were allegations made in court documents that the division allowed felons to vote. This was a direct result of a data match performed using the Sex Offender Registration Central Registry and the statewide voter registration list by a third party. Names that appeared to be a match, based on criteria unknown, identified that there were registered voters whose names were on the Sex Offender Registration Central Registry and that some of these individuals voted in the 2010 general election. The division did not receive any names of potential felon voters from a third party.

An individual who has been convicted of a crime that requires registration with the Sex Offender Registration Central Registry may remain on the registry for an extended period of time, up to life. Being named on the list doesn't preclude those individuals from registering to vote, as long as they have been unconditionally discharged from their conviction.

When an individual has been unconditionally discharged from incarceration, parole and probation, they are eligible to register to vote.

As of March 31, 2011, there are 6,107 voters inactive due to felony conviction and 1,271 voters inactive who have been unconditionally discharged but have not re-registered to vote.

To ensure that felons who are ineligible to vote, do not vote, the division will ensure that a data match between the Department of Corrections and the state voter registration file is conducted immediately prior to each election.

II. (D) MOVE Act Compliance

1. Election Dispute

Question: Does the interval between Alaska's primary and general election allow compliance with the MOVE Act in case of an election dispute, when primary results can be delayed by law, and general election ballots must be mailed 45 days before an election?

Federal law (MOVE Act) requires that ballots for the 2012 primary and general election must be mailed to Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voters no later than 45 days prior to a federal election.

The difficulty with meeting this mailing deadline for the primary election revolves around the candidate withdrawal deadline. Currently, a candidate may withdraw up to 48 days prior to the election. This allows the division only three days to print and mail ballots for the primary election.

The division was able to meet the 45-day ballots mailing time for UOCAVA voters during the 2010 General Election. However, it was extremely difficult and could have been derailed by factors outside the division's control.

It is recommended that legislation change the date of the primary election; change the candidate withdrawal deadlines for the primary and general elections; change the party replacement deadlines for the primary and general elections.

These changes will allow the state to more reliably meet the 45-day ballots mailing requirement for UOCAVA voters.

2. Electronic Voting

Question: With the passage of the MOVE Act, should Alaska eliminate the 60-day special advance ballot and expand electronic voting to allow the division to transmit blank ballots to voters?

The division should eliminate the 60-day special advance ballot for UOCAVA voters but continue to send to those voters residing in remote areas of the state and those traveling and working outside the United States.

The MOVE Act requires the division to send ballots electronically to voters, if requested by the voter.

Currently, the regulatory definition of electronically transmitted ballots is by facsimile machine. However, this is an antiquated method of electronic voting. In a review of the

legislative committee history for HB42, which implemented electronic transmission of ballots, it is clear that the intention of the statute's use of the term "electronic transmission" was meant to allow the division to use whatever means is modern and available. The bill was intended to make use of modern technology to encourage people to vote.

The use of fax machines is no longer considered modern technology. There are effective and secure ways to electronically transmit a ballot to voters. Many states implemented these types of procedures during the 2010 general election.

The division is continuously being asked by voters (both UOCAVA and non-UOCAVA) if they can receive their ballot by email.

The division is researching secure electronic ballot transmission methods. The recommendation is to amend state law to allow for this opportunity.

II. (F) Requirement to Show ID and Citizenship

Question: Should voters be required by law to show their ID, and what proof of citizenship should be necessary to register?

State law currently requires voters to present ID prior to voting. If the voter is personally known to an election worker, ID does not need to be shown.

Some Alaskans have urged a proof of citizenship requirement to register to vote. Today, Alaska requires a prospective voter to sign an affidavit attesting to his or her citizenship in the United States and in the State of Alaska.

If information is received that a voter is not qualified because they are not a U.S. citizen, the division requests verification of U.S. citizenship through the voter and/or the Immigration and Naturalization Service. If it is found that the voter is not a U.S. citizen, the division will inactivate the voter registration record.

Proof of citizenship is a sensitive area. In October 2010, Ninth Circuit Court of Appeals (*Gonzales v. Arizona, 624 F.3d 1162, 9th cir. 2010*) ruled that the Arizona Division of Elections could not require documents proving citizenship for new voter registrations. The court ruled that this violates federal law. The National Voter Registration Act (NVRA) allows voters to register without documentation but stipulates that lying about citizenship is perjury. The case is not resolved by the courts, but could have implications in Alaska. The division and the Department of Law will continue to monitor proceedings carefully.

When a voter registers to vote before a registrar, they must show identification. If no identification is provided, the registrar notes on the registration form that no ID was presented. When the division processes this form, the voter's identity is verified through the Division of Motor Vehicles (DMV) database and/or through a direct application between DMV and the Social Security Administration (SSA).

When a voter registers to vote by mail, their identity is verified through the DMV database and/or the SSA database.

If the identity of a voter who registered by mail or through a registrar without presenting ID cannot be verified through DMV or SSA, there is a notation made next to the voter's name on the precinct register that the voter must show identification. A voter who is personally known by an election worker cannot have the identification requirement waived if this notation is next to the voter's name on the precinct register.

II. (G) Election Contest – Certification

Question: Should the ground rules for defining an election contest be revised, since we've learned in 2010 that an election can be challenged before certification takes place?

Under Alaska State Statute, any defeated candidate or ten qualified voters may request a recount. The recount application must be received within five days following the completion of the state review board. The deadline for a recount involving a gubernatorial race is three days.

Currently, the statute regarding the timeline for bringing an election contest action says: "The action may be brought in the superior court within 10 days after the completion of the state review" (AS 15.20.550). Technically, an election contest action may be brought before certification now, so long as it is brought after state review. AS 15.15.440 sets out the process for state ballot review, and then AS 15.15.450 sets out the process for certification of the election after ballot review.

Election contest actions are entirely delineated in statute, so a change could be made, but the question remains whether it makes sense to make a change. The division needs to have the state review of an election complete so there is an official election result for the plaintiff to challenge in an election contest action.

Joe Miller challenged a state election in federal court. The federal court delayed state certification and neither the State of Alaska nor the state courts had control to lift the stay. The federal court did not "toll" or delay Mr. Miller's right to seek a recount, and he missed the opportunity to do so.

The situation that arose with the 2010 U.S. Senate litigation could have cost the state representation in the U.S. Senate. Changing the recount, recount appeal and election contest timeline can be detrimental to ensuring that the state has representation at the state and federal level.

Question: Why weren't all ballots counted by hand?

There were public comments received regarding the request by Joe Miller to have a hand-count of ballots for the U.S. Senate race. The process that took place regarding the write-in votes was solely for the purpose of determining how many votes were received by each write-in candidate from the total number of write-in votes cast. If Mr. Miller had requested a recount of the U.S. Senate election, it would have been granted; however the division never received such a request and therefore never conducted a recount.

As a matter of course, when a recount is requested, it is conducted by using the optical scan ballot tabulation equipment. The equipment is programmed to reject any ballot that is overvoted (more than one oval filled in) or undervoted (either entirely blank for the race being recounted or a mark that is too light for the tabulator to read). When a ballot is rejected it is placed in a box to be reviewed by the director. The director makes a decision whether or not to count the ballot and either party involved may challenge the decision. The challenged ballot is then sealed in an envelope to be preserved if it needs to be reviewed by the courts.

Each ballot is reviewed by observers and all ballots are subject to challenge.

During a recount, one precinct from each house district is randomly drawn for a hand-count verification.

To avoid confusion in the future, the division will post on their website the date the state review board has completed their review, which will indicate to candidates and voters that a recount request must be made within five days of that date.

There were also public comments received regarding the hand count verification process. This is a process in which one randomly drawn precinct that accounts for at least five percent of the total votes cast for the district is hand counted. If there is a discrepancy of greater than one percent, the entire district is recounted by hand. In the four years this requirement has been in statute, there has never been a need to recount the ballots for an entire district. Following the hand count verification from the 2010 General Election, copies of the paperwork were provided to observers from the Miller campaign.

II. (H) Voter Assistance

Question: What voter assistance is allowable?

Both state and federal law require that a voter be provided assistance at any time throughout the registration process and voting process. There are no limitations as to what level of assistance may be provided if requested by the voter.

Language assistance is specifically required by federal law.

The division provided, at voters' request, a list of qualified write-in candidates. Initially, an absentee voting site erroneously posted the list. Once the division learned about it, the list was immediately removed. Seventeen voters voted during the period the list was posted. These ballots were kept segregated, counted, and returned to their envelope in case of any future challenge. There were no challenges made to these ballots

The Alaska Democratic Party and the Alaska Republican Party filed a lawsuit against the division to prohibit the use of the write-in list. The Alaska Supreme Court upheld the use of the list ruling that it was consistent with Alaska's voter assistance statutes and did not violate state election regulations.

Public comments were received which stated that numerous ballots appeared to have the name of a write-in candidate written by the same person. Nothing in state law prohibits an election worker from assisting a voter with the writing of a candidate's name. This is an allowable form of voter assistance.

A number of write-in ballots were challenged due to similar handwriting. No evidence was presented to indicate this was the result of anything other than voter assistance or common penmanship among voters. This issue is also part of the complaint in current, active litigation in Perry et al. v. LG, SOA, 4FA-11-973 CI. Due to the past and current litigation, this report makes no recommendation on this issue.

Question: Is voter assistance documented?

The division does not instruct poll workers to document when a voter receives assistance, with the exception of language assistance. The division instructs poll workers, when requested, to provide any necessary voter assistance. The only type of assistance that is documented is the number of language assistance requests and the type of language. Poll workers are instructed to maintain a language assistance log. Voter names are not maintained on the log. The language assistance log is a method used by the division to determine where language assistance, especially Alaska Native language assistance, is needed to ensure there are bilingual poll workers in those areas.

II. (I) Public Information to Update Voter Lists

Question: What information on voters may be used to update voter lists?

Changes to a voter's residence address must be provided in writing by the voter.

Mailing address changes (not residence addresses) can be made based on information received from the USPS or based on information provided by the voter to the Permanent Fund Dividend program.

A voter's record may be inactivated when information is received from another state indicating that the voter is now registered in their state.

A voter's record may also be inactivated as a result of information received from the Division of Vital Statistics and the Department of Corrections.

The division has been following the "Upgrading Democracy Project," by PEW Center on the States. We have been invited, through this project, to compare voter registration lists with a wider array of data sources to broaden the base of information used to update and verify voter rolls. To participate, the State would need to share data Alaskans provide to the Division of Motor Vehicles. We have also been asked to share data from Permanent Fund Dividend records because voters have every reason to keep address records with the PFD division current. The division currently has access to PFD information but does not have complete access to DMV information that would further help verify our registration records, or further reach out to eligible citizens who are not registered to vote. The Division is considering the possibility of joining the "Upgrading Democracy Project," but it will not do so unless the privacy of Alaskans' personal data can be assured.

II. (J) Information on Who Has Voted

Question: Can we offer "real-time" updates on which voters have voted?

At this time the division does not offer a "real-time" or electronic update identifying which voters have voted. Nor does the division offer an hourly "carbon copy" of voters signing in to vote, as some other states do.

Poll watchers typically track this information on paper lists which match the list of voters for a specific precinct. They check off the names of voters as they vote and provide that information to campaigns and/or political parties. However, poll watchers are not allowed to see the registration rolls and can only glean voter information by listening.

The division will consult with a third party to research a "real-time" voter history system and a cost/benefit analysis of such a system.

II. (K) Party Participation and Access

Question: How do we ensure that political parties have full participation in and access to the election process?

The election process is open to all political parties, candidates, and the public. They have access to voter lists, absentee lists, and a presence at the review of absentee and questioned ballots, as well as the counting of these ballots.

The political parties are asked for names of individuals to serve as workers at polling places and as members of the state review board.

There are a large number of non-partisan and undeclared voters in the state. The division ensures that a board is not composed of only one party or another, but strives to ensure there is a combination. There are some precincts that may not have a worker that is registered as Republican or Democrat, but there are never boards that are entirely composed of only one party. There were occasions in 2010 when a board was composed of entirely non-affiliated workers.

Public comments were made stating that the division does not provide parties adequate notice regarding election worker and board appointments. The division will improve communication with the parties regarding election worker recruitment deadlines by providing multiple notices to them.

2010 Election Review
III. Department of Justice Review

Alaska, and all political subunits (boroughs, cities, school districts), are subject to the provisions of Section 5 of the Voting Rights Act. This section requires the state to obtain preclearance from the U.S. Department of Justice (DOJ) for any change affecting the voting process before the change is implemented.

Routine preclearance submissions requested by the division include changes to polling locations, precinct boundaries, regulation changes, legislative changes and changes to forms used by the division such as the voter registration application, absentee ballot application, voting instructions and posters.

DOJ has 60 days after receiving a preclearance submission to make any objection to the voting change.

III. (A) Examples of Changes Needing Preclearance

Changes affecting voting include, but are not limited to, the following examples:

1. Any change in qualifications or eligibility for voting.

2. Any change concerning registration, balloting and the counting of votes, and any change concerning publicity for or assistance in registration or voting.

3. Any change with respect to the use of a language other than English in any aspect of the electoral process.

4. Any change in the boundaries of voting precincts or in the location of polling places.

5. Any change in the constituency of an official or the boundaries of a voting unit (e.g., through redistricting, annexation, deannexation, incorporation, reapportionment, changing to at-large elections from district elections, or changing to district elections from at-large elections).

6. Any change in the method of determining the outcome of an election (e.g., by requiring a majority vote for election or the use of a designated post or place system).

7. Any change affecting the eligibility of persons to become or remain candidates, to obtain a position on the ballot in primary or general elections, or to become or remain holders of elective offices.

8. Any change in the eligibility and qualification procedures for independent candidates.

9. Any change in the term of an elective office or an elected official or in the offices that are elective (e.g., by shortening the term of an office, changing from election to appointment or staggering the terms of offices).

10. Any change effecting the necessity of or methods for offering issues and propositions for approval by referendum.

11. Any change affecting the right or ability of persons to participate in political campaigns which is affected by a jurisdiction subject to the requirement of Section 5.

III. (B) Pending Changes Needing DOJ Review

1. As a result of the creation of a new political group, the Alaska Constitution Party, and the removal of the political group, the Moderate Republican Party, the division is in the process of updating the procedures relating to the voter registration application, absentee ballot application, primary ballot choice poster and the voter identification card to reflect the political group changes. Once these forms are updated, they will have to be submitted to DOJ for preclearance.

2. Any change to Alaska Statutes or regulations relating to counting write-in votes or the rules of counting write-in votes, including voter intent will, need to be precleared by DOJ after passage and prior to implementation.

3. Any change to Alaska Statutes, regulations or forms relating to candidacy declaration requirements, including write-in candidates, will have to be precleared by DOJ after passage and prior to implementation.

4. Any change to Alaska Statutes relating to the date of the primary election will have to be precleared by DOJ after passage and prior to implementation.

5. Any changes to Alaska Statute and/or regulation for compliance with the MOVE Act will have to be precleared by DOJ after passage and prior to implementation.

6. Any changes to Alaska Statute and/or regulation relating to requirements for voter identification or for proof of citizenship to register will have to be precleared by DOJ after passage and prior to implementation.

7. Redistricting changes, including changes to precinct boundaries, must be precleared by DOJ after adoption and prior to implementation.

III. (C) Meeting with DOJ Personnel

Lieutenant Governor Treadwell and the Director of the Division of Elections met with staff from the Department of Justice in Washington, D.C. on February 10, 2011 to discuss various Voters' Rights Act issues applicable to Alaska.

1. **Preclearance**

The Alaska delegation expressed appreciation for DOJ's cooperation in quickly preclearing the write-in list process for the 2010 General Election.

2. **The MOVE Act**

Alaska had initially thought it would not be able to meet the 45-day deadline for ballot distribution set out in the MOVE Act. The state had applied for a waiver from this requirement of the Act, and that waiver was denied. Division staff then worked with DOJ to find a way to comply with the MOVE Act, and DOJ's guidance was greatly appreciated in finding a solution to allow Alaska to meet the ballot distribution deadline.

3. **Bail Out**

The term "bail out" refers to the process by which covered jurisdictions may seek exemption from Section 5 coverage. In order to bail out, a covered jurisdiction needs to obtain a declaratory judgment from the District Court for the District of Columbia.

The bail out standard requires that a covered jurisdiction demonstrate nondiscriminatory behavior during the ten years prior to filing, and while the action is pending that it has taken affirmative steps to improve minority voting opportunities.

Discussion took place regarding the bail out process. DOJ clarified that the state may not apply for a bail out from the Voting Rights Act for ten years after the date that federal election observers are no longer in the state. The state received confirmation that it is not entitled to receive copies of the federal observer reports, as these reports are not subject to the Freedom of Information Act. On October 1, 2009, the Bethel Census Area was certified for federal observers, and to date observers have been present for state elections only in Bethel.

4. **Pending State Legislation**

DOJ was informed that there is legislation pending relating to elections and that the state, as always, would be submitting the legislation for preclearance prior to implementation. Clarification was received that if DOJ does not grant preclearance to a change in statute, the existing statute would remain in force.

5. **Minority Language Assistance**

DOJ is interested in seeing the state expand language assistance into more areas of the state and work towards strengthening the Inupiaq language assistance program.

2010 Election Review
IV. Issues for Third Party Review

Status of election security study recommendations

In 2007, then Lieutenant Governor Sean Parnell and the Division of Elections requested the UAA to conduct a study of Alaska's election security. Phase I of the study included a review of security studies conducted by other states and provided for a preliminary assessment of Alaska's election system. Phase II of the study provided for a detailed evaluation of Alaska's election system to provide recommendations that would strengthen both the technology and election procedures to mitigate any known security risks.

In evaluating Alaska's election system, the University reported that Alaska's election system is among the most secure in the country and is in good shape. In Phase II, the University provided several recommendations to further improve the security of Alaska's election system. The recommended changes were broken into two categories: changes recommended prior to the 2008 elections and changes recommended after the 2008 election.

Below is the status of each recommendation included in Phase II of the report:

IV. (A) Pre-election Recommendations

1. **Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code**

   The division implemented the use of a hash code validation for all GEMS computers. This validation ensures that all GEMS computers are using the correct, registered code associated with the current software version. In addition, the GEMS computers are not connected to a network or internet and access to these computers is restricted to authorized personnel only.

2. **Install new software that allows election officials to create a more secure password authentication system for touch-screen machines**

   The division purchased and implemented the use of Key Card Tool which allowed the division to create their own authentication password and encryption keys for the touch screen units.

3. **Change passwords on all voting technology throughout the system**

   The division implemented procedures to change passwords on all hardware and software, including the BIOS, Windows and GEMS election database login passwords. The documented passwords for all systems are stored in a key safe in the director's office.

4. **Use tamper-evident seals on shipping cases and envelopes**

   Prior to 2008, the memory cards used in the touch screen units were installed in the units prior to shipping. In 2008, the division implemented a policy that memory cards would be shipped separately from the unit in tamper evident envelopes. The division determined that since the units were not shipped with the memory cards installed, the division deemed that tamper-evident seals on shipping cases were not necessary.

   In addition to tamper-evident seals on memory card envelopes, tamper-evident seals were placed on all voting equipment. One seal was placed on the optical scan unit that covered either the front or back seam and pre-drilled hole. One seal was placed on the touch screen unit that covered the seam and pre-drilled hole on the back of the machine. Division staff recorded the seal number used on each piece of voting equipment.

5. **Add election security material to poll workers' training manuals.**

   Additional instructions were provided to election workers on equipment security that included a check list and procedures for seal inspection and what to do if the seal was broken. In addition, the division implemented the use of a security log for each piece of equipment. The log listed the tamper-evident seal number, instructions for inspection and a sign-off area for the election workers to sign and return to verify the seal number matched the number provided and that the seal was unbroken.

6. **Increase security procedures in absentee polling locations**

   The division does not use voting equipment in absentee polling locations. The touch screen voting units used in the regional offices early voting stations were handled with the same security measures as the equipment used in the polling places. Absentee voting officials were provided with instructions on maintaining the security of their ballots and voting materials.

7. **Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines**

   The division purchased optical scan units for the precincts in the North Slope Borough and initiated use of the units in the 2008 elections.

IV. (B) Post-election Recommendations

1. **Upgrade voting machines and other technology to improved platform: Assure 1.2**

   Assure 1.2 was federally certified by the United States Election Assistance Commission in August 2009. The division chose not to upgrade to Assure 1.2 for the 2010 General Election because the system provider, Premier Election Systems, was in the process of being acquired by Election Systems & Software (ES&S) which triggered an anti-trust violation investigation. This acquisition led to another vendor, Dominion Voting, obtaining the rights to the Assure 1.2 platform. Working with Dominion Voting, the division has begun the process to upgrade their ballot tabulation system to the Assure 1.2 platform. The upgrade will be completed in 2011.

2. **Establish long-term security goals and a method for measuring progress**

   The long-term security goals established by the division relate to the recommendations provided in the study. It is the policy of the division that the recommendations and improvements made for the 2008 election cycle will be maintained for all future elections unless other security issues are identified and addressed.

3. **Improve testing processes to ensure that all voting technology is functioning properly and recording votes accurately**

   The division adopted the University's increased scope of recommended logic and accuracy testing for the 2008 and 2010 election cycles. Memory cards used in the touch screen units were tested using a combination of an automatic and manual testing function. Memory cards used in the optical scan units were also tested following recommended test procedures. The State Ballot Review Board and the Regional Accu-Vote Boards and/or Accu-Vote Coordinators tested the memory cards. In addition to the memory card testing, a functionality test was conducted on all voting equipment used in the election to ensure the equipment was functioning properly prior to use during the election. The improved functionality, logic and accuracy testing performed by the division will be maintained for future elections.

4. **Develop and implement a standard plan for tracking and changing passwords**

   The division has implemented a standard to change all applicable passwords prior to the start of a statewide election cycle. Documentation of the passwords is maintained in a safe in the director's office.

5. **Improve system for tracking the number and location of voting machines, through barcodes or other inventory control measures**

   The division implemented a consistent inventory management system statewide. All offices are tracking voting equipment in a uniform manner.

6. **Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry**

   A separate locked key safe in the director's office is used to store keys and password codes. The other division offices where equipment and keys are stored maintain physical security features such as alarms and dead-bolts.

7. **Buy more secure shipping containers for optical-scanners**

   The division increased the number of secure shipping containers for optical scan units during the 2008 election cycle, compared to previous elections. If additional containers are needed, the division will ensure an adequate supply is on hand for in the future.

8. **Recruit and train more poll workers**

   The division consistently strives to train all poll workers prior to each election cycle. The division had tremendous success during the 2008 and 2010 elections by having an adequate number of poll workers at each precinct. New security procedures were added as a component to the division's training for the 2008 and 2010 elections.

9. **Consider partnerships with other institutions to conduct ongoing evaluation and implementation of improvements in election security technology**

   The division believes that the implementation of the recommendations from Phase II of the UAA Study significantly increased the public's confidence in the integrity and accuracy of the election process and voting technology. The UAA Study is discussed fully in section IV of this report.

   As part of the election certification process, the division performs a hand-count verification of 5% of the ballots cast at the polls in each of the state's 40 house districts. The hand-count of the 2008 and 2010 election results verified that the state's ballot tabulation system accurately counted and reported election results.

10. **Third Party Review**

    In addition to the election security study, the division partnered with UAA Institute of Social and Economic Research to assist with outreach and improvements to the division's Yup'ik language assistance program. The division has benefited from these partnerships and will continue to pursue further partnerships.

    One specific area needing further research and partnership is a review of the division's post-election processes, including a review of the division's audit procedures and hand-count verification of election results. Public comments were received relating to audit standards. In addition, comments continue to be received relating to the accuracy and security of the division's ballot tabulation system.

Although the UAA election security study concluded that Alaska's election system is among the most secure in the country and has a number of safeguards, the study did not include a thorough review of post-election processes used by the division and used in other jurisdictions across the country.

Alaska is known for close elections and recounts. A thorough review of the post-election processes, including any recommended changes, will enhance the public's trust in Alaska's election system.

Other areas to be included for third party review are:

a) New review of ballot security issues
b) Audit to ensure that non-U.S. citizens are not voting
c) Audit to ensure that felons are not voting
d) Explore systems or methods that can provide for real-time voter history

2010 Election Review
V. Miscellaneous Public Comments

During the 2010 General Election review, Lieutenant Governor Treadwell solicited comments and input from the public, political parties and candidates. Information relating to the types of comments received were included throughout the election review in appropriate areas.

There were additional comments received that do not relate to a specific subject addressed in the report. A summary and response to those comments follows:

V. (A) Create a better environment for the military to vote

In 2000, the Department of Defense (DOD) issued a directive that polling places could not be established on military bases. At that time, the Division of Elections had established polling places on both Eielson Air Force Base and Fort Wainwright. Working through the late Senator Ted Steven's office, the division was able to maintain polling places on the military installations for the 2000 election cycle but was informed they would have to be moved for the 2001 municipal elections. The polling places for both installations were moved to off-base locations in 2001.

In 2003, the division was notified that DOD issued new election guidance indicating that if an installation facility had been designated as a polling place as of January 1, 1996 through December 31, 2000, the installation commanders could not deny the use of that facility as a polling place.

For the 2004 elections, the division investigated moving the polling places back onto both installations. Because the precinct boundaries for both installations include non-military voters, the division decided not to move the polling place back to the installations because non-military voters would have difficulty accessing the polling places.

The division suggests that under the new redistricting plan, the precinct boundaries be changed so that only installation boundaries are included in the precinct. When a precinct is wholly contained within the installations, the division can once again work with the military to establish polling places on the bases. This report recommends this change to the Redistricting Board.

V. (B) Provide notice of any change in practice or procedure

If the division decides to change a practice or process, ample notification of that change will be given.

The division follows the Administrative Procedures Act to adopt new regulations. Statutory changes can only be achieved through the legislative process. All changes that affect voting are sent to the U.S. Department of Justice for preclearance.

There are some internal policies that require emergency action and preclude prior public notice.

In order to improve public notification, the division will add a notice section to its website and post notices of public interest, such as filing deadline dates, withdrawal deadlines, and state review board dates. The election year events are captured on the public election calendar which is available on the division's website: http://www.elections.alaska.gov/doc/forms/H11.pdf.

V. (C) Open primary

The division does not have the authority to change the primary election structure. Only the legislature has that authority. The current primary election structure is a result of many years of litigation. Title 15 Of Alaska State Statute affirms that political parties have the right of freedom of association and can determine which candidates will appear on their ballots and which registered voters will have access to their party's ballot. These determinations are documented and codified in the political party by-laws. Party members who meet candidate qualifications are allowed to appear on the party primary ballot.

The history of Alaska's primary election has been influenced by litigation over primary elections, some of which reached the United States Supreme Court. On June 26, 2000, in California Democratic Party v. Jones, the U.S. Supreme Court ruled that California's Blanket Primary violated political parties' First Amendment right of freedom of association. The court said political parties have the right to offer voting to self-identified members and not to the general electorate. At the time, Alaska's primary election was similar to California's primary election and thus the Jones case ruling also invalidated parts of Alaska's primary election law.

To comply with the Jones case ruling, the State of Alaska adopted emergency regulations that allowed the 2000 Primary Election to be conducted as a Party-Rule Ballot Primary.

During 2001 legislative session the Alaska State Legislature passed legislation that specified a primary election ballot was required for each political party in SCS CSHB 193(FIN).

Shortly after the 2002 General Election, the Green Party and Republican Moderate Party filed suit, challenging the requirement of separate party primary ballots. In 2005, the Alaska Supreme Court, in Green Party et. al. v. State of Alaska et. al. prevented the state from enforcing the provision in election law requiring separate party primary ballots. This ruling affirmed the earlier superior court ruling which allowed parties to decide if they wanted to appear on a Combined Party ballot. Parties were required to provide information to the state if they wanted to appear on the Combined Party ballot and indicate which voters would have access to their ballot.

In response to the Green Party case ruling, the Republican Party chose to include only Republican candidates on its primary ballot and provide ballot access to only those voters registered as republican, nonpartisan or undeclared.

As an initial response to the Green Party case ruling, the Alaska Libertarian Party, Alaskan Independence Party, Republican Moderate Party, and the Green Party of Alaska agreed to be on a combined ballot that would be available to all registered voters. (Both the Green Party

and the Republican Moderate Party lost recognized political party status as a result of the 2005 ruling allowing the Combined Party Primary ballot.)

Currently, the Alaska Democratic Party appears on a ballot with the Alaskan Independence Party, and the Alaska Libertarian Party. Any registered voter may have access to this ballot.

V. (D) Ballot counting machines can be hacked

As previously mentioned in Section IV of the report, UAA conducted a study of Alaska's election system and found that the state's election system is among the most secure in the nation. Unlike other studies conducted, the UAA study examined not only voting technologies but also policies and procedures that add to the security of the system. UAA found that there are multiple steps, procedures and security features that make the system safe and provided recommendations to further improve the security of Alaska's election system.

To date, the division has implemented all but one of UAA's recommendations and will have the recommendations fully implemented in 2011. The final recommendation for implementation is for the division to upgrade the ballot tabulation system to the Assure 1.2 platform, which will address many of the security risks identified with the state's ballot tabulation system software (GEMS). The security recommendations provided by UAA and adopted by the division, along with the Assure 1.2 upgrade, will continue to ensure that Alaska's election system is secure. In addition, performing the hand-count verification of election results will continue to ensure the system is accurate.

V. (E) Faxed ballots are transcribed – precautions to prevent fraud

Under both state and federal law, the division must provide for electronic voting. Blank ballots are transmitted to voters via fax machine. Once voted, the ballot can be returned by mail or fax.

An electronically transmitted ballot, whether mailed or faxed, cannot be counted by the division's optical scan counting equipment because it is on plain paper, not on official ballot stock.

6AAC 25.065 allows the bi-partisan absentee ballot review board members to produce a facsimile ballot that exactly indicated the candidates chosen by the voter using ballot stock that can then be read by the optical scan tabulator.

When producing facsimile ballots, one person marks the ballot while another person, of a different political party, verifies the ballot was marked correctly. This ensures that the facsimile ballot is marked for the same candidates as the original ballot. Any observer present during the review is allowed to review the ballot.

If a facsimile was not produced for faxed ballots, the ballots would have to be hand-counted. The division believes this would impact the amount of time it takes to count and report election results. The division will monitor new methods to allow machine counting of ballots received by electronic means.

V. (F) Special Advance Ballots

State law requires the division to send a special advance ballot to any registered voter who notifies the division they are living, working or traveling outside the United States at the time of the election, or in a remote area of the state where distance, terrain, or other natural conditions deny the voter reasonable access to a polling place at the time of the election.

This ballot must be sent starting 60 days prior to each state primary, general or special election.

Because the candidate withdrawal deadline has not yet occurred (48 days prior to an election), the ballot is printed with only race headings and a blank line for the voter to write the name of the candidate they wish to vote for. Each voter is sent a list of certified candidates and instructions on how to vote their ballot.

For a general election, the special advance ballots are sent prior to the election being certified. Therefore, a candidate list is sent containing the names of all candidates that appeared on the primary election ballot. The voter is given information regarding the candidate list, that the election has not yet been certified, therefore not all candidates appearing on the list will have advanced to the general election ballot. They are given the option of voting by political party as well as by candidate name.

As prescribed in state election law, Lisa Murkowski remained an official candidate and her name remained on the special advance candidate list until the election was certified.

All voters receiving a special advance ballot are also sent the official ballot once it is available. Voters are instructed to vote and return both ballots. The division will count the official ballot if received timely. If the official ballot is not received in time by the division, but the special advance ballot is, the division will count the special advance ballot.

To comply with the MOVE Act, the recommendation is for a change in state statute to allow the division to mail special advance ballots 45 days prior to each election to all UOCAVA voters and voters working or traveling outside the U.S. and those in remote Alaska.

V. (G) Use of stickers on ballots

Since the division implemented the current ballot tabulation system, the use of stickers has been prohibited by state law.

The division has recently spoken with representatives from the division's ballot tabulation equipment provider. There is presently no voting equipment manufactured or certified that accommodates the use of stickers. Vendors do not recommend their use because of potential damage to equipment and the potential for miscalculations of votes for not only the write-in candidates but other candidates as well.

2010 Election Review
VI. Conclusion

Once again, thank you to all Alaskans for their contributions to this report.

State of Alaska
Election Security Project:
Election Process Review
Phase 3 Report

Appendix C: State of Alaska Election Security Project Phase 2 Report (2008)

UNIVERSITY
of ALASKA
ANCHORAGE

State of Alaska Election Security Project

Phase 2 Report

Prepared for Lieutenant Governor Sean Parnell
and the State of Alaska Division of Elections

May 16, 2008
Final Report

This page left intentionally blank

Executive Summary
Alaska Election Security Report, Phase 2

See the back page for a list of contributors

University of Alaska Anchorage April 2008

Alaska's election system is among the most secure in the country, and it has a number of safeguards other states are now adopting. But the technology Alaska uses to record and count votes could be improved—and the state's huge size, limited road system, and scattered communities also create special challenges for insuring the integrity of the vote.

In this second phase of an ongoing study of Alaska's election security, we recommend ways of strengthening the system—not only the technology but also the election procedures. The lieutenant governor and the Division of Elections asked the University of Alaska Anchorage to do this evaluation, which began in September 2007.

The Division of Elections itself first identified a number of possible security improvements, and we evaluated their feasibility and potential benefits. We also identified additional improvements.

The table shows our main recommendations, dividing them into changes the state could make before the 2008 primary and general elections and changes that would take longer to put into effect.

The biggest recommendation is that the state upgrade all its technology to a new system recently developed by Premier Election Solutions, which manufactures the voting machines and related technology Alaska and other states use.

That new system is important. It corrects a number of vulnerabilities in the current system, identified in Phase 1 of this study. But as of April 2008, it had not yet been certified to standards required by the federal Election Assistance Commission. Alaska can't use the new system until it is certified—and when it is certified, it will take a lot of time, money, and people to do the upgrade. It will have to be installed on hundreds of optical-scanning machines, touch-screen devices, election-management servers, and other equipment scattered throughout Alaska. Taking on such a big, expensive job would not be practical, even if the new system were certified in the next few months. At this point, the Division of Elections is already doing many tasks required before the primary election in August and the presidential election in November. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well.

But between now and the election, the state can improve security, with the changes recommended below. After the election, it can upgrade to the new system and develop a method for continuously monitoring changes in technology. We also recommend improving the way voting equipment is transported, tracked, and stored—as well as increasing the number of poll workers and providing them with more training in election security.

Recommendations for Improving Alaska's Election Security

Change By 2008 Election	Why?	Change After Election	Why?
✔ *Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code*	This series of changes in technology and election procedures will make the existing technology more secure; improve security procedures among election officials and poll workers; and help increase Alaskans' confidence in the integrity of state elections. These measures can all be taken in the short-term, before the August primary and the November 2008 election.	✔ *Upgrade voting machines and other technology to new, improved platform*	Installing the new platform is the single-most important change the state can make, because it will reduce or eliminate risks of vote-tampering identified in the current system. But the platform must first be certified to the Election Assistance Commission's 2002 Voting System Standards, and after that will require an estimated 1,000 man-hours to install on election equipment statewide. Even if it were certified soon, it is not practical now to install the upgrade before the 2008 elections, given the time, expenses, and logistics involved. The other post-election recommendations are either longer-term enhancements of measures recommended for 2008, or additional security measures that there isn't time enough to implement before the 2008 elections.
✔ *Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines*		✔ *Establish long-term security goals and a method for measuring progress*	
✔ *Change passwords on all voting technology throughout the system*		✔ *Improve testing processes to insure all voting technology is functioning properly and recording votes accurately*	
✔ *Use tamper-evident seals on shipping cases and envelopes*		✔ *Develop and implement a standard plan for tracking and changing passwords*	
✔ *Add election-security material to poll workers' training manual*		✔ *Improve system for tracking the number and location of voting machines, through bar-codes or other inventory-control measures*	
✔ *Increase vigilance about security procedures in absentee polling locations*		✔ *Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry*	
✔ *Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines*		✔ *Buy more-secure shipping containers for optical-scanners*	
		✔ *Recruit and train more poll workers*	
		✔ *Consider partnerships with other institutions to do ongoing evaluation and implementation of changes in election-security technology*	

What is the Current System?

This is a particularly appropriate time for this study, not only because election-security has become a prominent issue nationwide, but also because this year marks the tenth anniversary of Alaska's use of electronic voting technology.

Unlike other election-security studies, our study is examining not only voting technology but also policies and procedures that add to the security of the system.

Much of our work in the first phase of the study was assessing the existing election system. To provide background for our recommended improvements, here we first briefly summarize the existing system. The figures on this page and the facing page show how the current system is organized and how it works.

The lieutenant governor heads the election system, and the Division of Elections manages federal and state elections statewide. The state is divided into four election regions, which in turn have 439 precincts. Election regulations, procedures, training, and technology are the same throughout the state.

There are multiple steps in the voting process, from the time Alaskans go to the polls until the director of elections certifies the results (as the figure on the facing page details). The process includes a number of security features that make it among the safest in the country:

- A centralized voting system, with standard procedures and identical hardware and software throughout Alaska. This centralization minimizes opportunities for tampering and allows flaws identified in any part of the system to be corrected statewide.
- Paper back-ups for all votes. Although optical scanners do scan and count ballots in 290 of Alaska's 439 precincts, almost all Alaska voters mark paper ballots that serve as back-ups to electronic tallies. There are touch-screen machines in all precincts. Only about 1% of voters use those machines, which also have internal paper reels as back-ups.
- Independent verification and cross-checking of paper ballots and preliminary electronic results.
- Audit of machine-counts of votes by hand-counts in a random sample of precincts.
- Observers invited to watch both voting and vote-counting procedures.

What Makes a System Secure?

Alaska's system has many strengths, but there is room for improvement. Alaska and other states use electronic systems to count and record votes. That technology has a number of advantages—it makes counting votes much faster, for example. Federal law also requires all polling places to have touch-screen devices for voters who can't mark paper ballots.

But election-security studies in other states have shown that the same voting technology voting used in Alaska could be vulnerable to tampering. Alaska also has security issues most other states don't face. It is huge—375 million acres—and the road system covers only about 10% of the land area. More than a hundred small communities can be reached only by water or air. Storms and intense cold frequently disrupt travel and shipments to remote communities.

Alaska's Election System

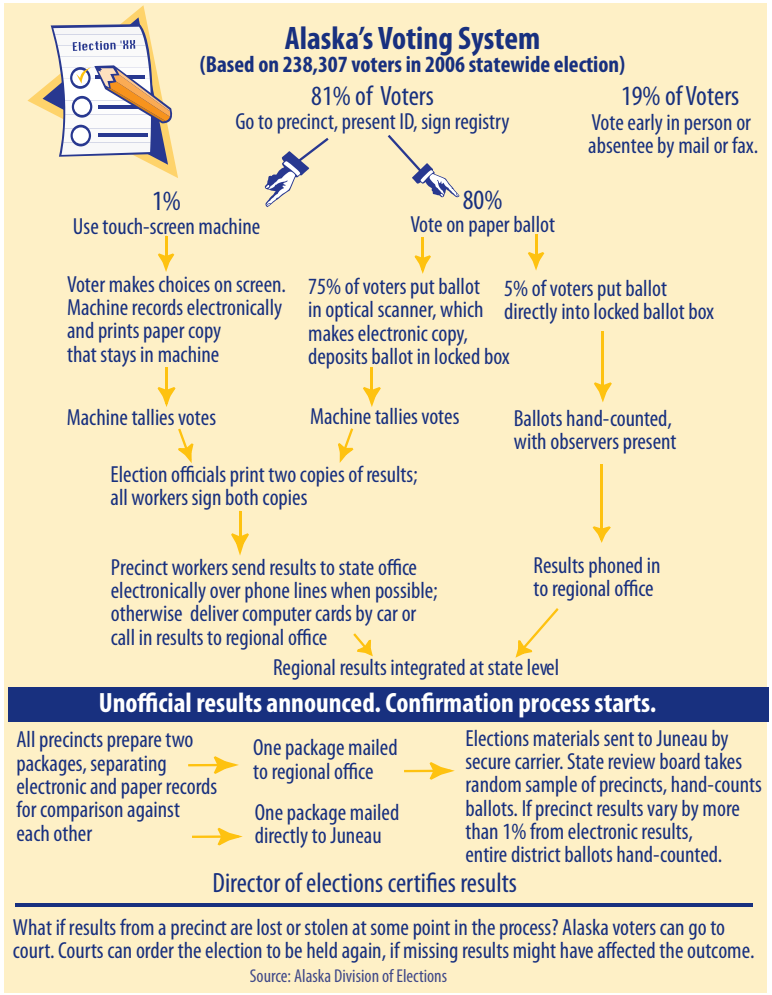
Lieutenant Governor	• Supervises Division of Elections • Appoints director of elections
Alaska Division of Elections	• Director of elections hires election supervisors for each region
Four Regions (Based on 40 House Districts)	
Regional Offices (Juneau, Anchorage, Fairbanks, Nome)	• Regional election supervisors hire bi-partisan election boards and supervisors for each precinct
439 Precincts (Large communities have multiple precincts)	• Precinct election chair-person hires bi-partisan election officials • Political parties, independent candidates, and groups sponsoring or opposing ballot initiatives may appoint observers to witness voting and vote-counting procedures

Source: Alaska Division of Elections

So sending ballots and election equipment to and from communities around the state, as well as storing equipment in small communities with limited facilities, is very expensive and poses many logistical challenges.

To evaluate how Alaska could improve security, we first thought about the elements that make a system secure, and grouped them into three categories: defense in depth, fortification of systems, and confidence in outcomes.

- *Defense in depth:* A secure system should have multiple layers of protection, so that if one fails others are still in place. This layered approach can discourage hackers, because they would have to take several undetected steps to penetrate the system's security. Also, layers can provide early warning of attacks in time for election officials to take action. Equipment, people, and procedures together provide defense in depth.
- *Fortification of systems:* This means making electronic systems as secure as possible and using the latest certified updates, which may correct vulnerabilities in earlier systems. Alaska uses optical scanners that tally votes cast on paper ballots; touch-screen machines with internal paper reels that record the votes cast; and servers that integrate and tally the electronic and hand-count results. All these system should be equipped with the latest updates to minimize the potential for votes to be miscounted or tampered with, and they should be protected so unauthorized users can't interfere with their operation before, during, or after elections. The systems must also be certified to federal standards and verified by independent testing centers.
- *Confidence in outcomes:* Systems and results have to be verifiable and shown to be reliable—to increase confidence of both voters and election officials in the system. The methods used to select a sample of results for hand-counting must also provide a high level of confidence. The election process must be open, so anyone can observe what is happening—and those who verify results must be objective and bipartisan.



Alaska's centralized processes and procedures at the state level make it easier to implement consistent security practices. Few states have such centralized systems, with standard practices and voting equipment statewide. Most states have decentralized systems—that is, systems in which counties, cities, or townships can set their own election procedures.

Also, Alaska's system provides a verifiable paper record of all the votes cast. Almost all voters mark paper ballots that are scanned and counted by an optical-scanner. About one percent of voters use touch-screen machines, with no paper ballots, but there is voter verifiable paper record .

The Pew Center for the States recently examined how many states have verifiable paper back-ups for votes. Keep in mind that most states have decentralized election systems—meaning individual counties or other local jurisdictions can choose their own methods—so the map illustrates the general rather than the exact situation in all states.

As the map shows, in 35 states all or most votes are backed up by paper records. In some of those states, voters mark paper ballots, which are then scanned and counted by optical scanners; in other states, voters mostly use touch-screen machines with internal paper reels.

But as of early 2008, 14 states primarily used touch-screen machines without paper reels. The Pew Center reports that two of those states—New Jersey and Maryland—have plans to implement paper-based systems. The remaining state, New York, still uses the lever-voting system, but almost all counties plan to begin using paper-based systems in 2009.

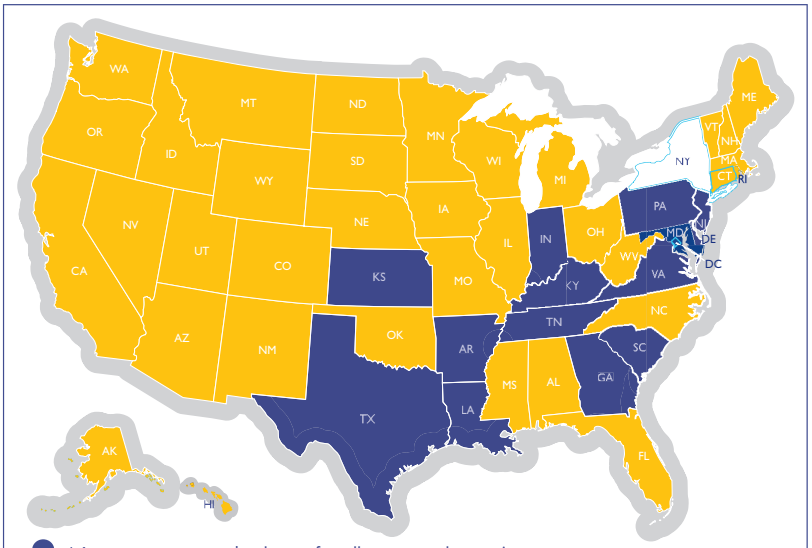
So overall the movement among states is toward systems with paper records—like the system already in place in Alaska.

How Did We Identify Security Issues?

- We studied the approaches taken in other states, to determine practices that could be helpful in Alaska.
- We evaluated the improvements the manufacturer of voting equipment has taken to correct security issues identified in other election-security studies and summarized in our Phase I report.
- We did a detailed, hands-on evaluation of storage, transportation, and packaging of election equipment and materials.
- We identified issues unique to Alaska, given our geographic diversity and transportation logistics.

We found that Alaska is well-positioned, compared with many other states. Alaska has in fact put into effect safeguards and processes that other states are now adopting to deal with election-security issues. But we also want to emphasize that every state faces different security and procedural challenges. There is no single solution right for every state.

We did find, however, that two aspects of Alaska's system help its election security, relative to that in other states: its centralization, and its paper ballot back-ups for virtually all votes.



14 states, no paper-back-ups for all or most electronic votes

35 states, some form of paper back-ups for all or most votes

1 state, lever-voting system

Notes: Many states use more than one voting technology. Not all states that have some paper back-up have complete paper back-up. New Jersey plans to have paper back-ups before the 2008 election; New York plans to adopt a paper-based system in 2009; Maryland law requires paper back-up by 2010.

Source: Based on Pew Center for the States, 2008

What Do We Recommend?

The table on the front page summarizes our main recommendations, some of which the Division of Elections could put into effect before the August primary and the November general election, and some of which it can't. Here we explain more about some of the most important recommendations, which are discussed in detail in the full report.

- ***Upgrade to the new, more secure platform after the election.*** We can't over-emphasize the importance of this upgrade. Alaska, California, Florida, and other states use the same or similar voting technology. Election-security studies in several states found that the existing technology was potentially vulnerable to vote-tampering in a number of ways. The new platform, (Premier Election Systems Assure 1.2), which the manufacturer developed in response to those studies, is still being tested to insure that it meets standards set by the federal Election Assistance Commission. We had hoped the system could be installed on Alaska's voting equipment by the 2008 election, but we now believe that's not feasible. Alaska is now in the run-up to the August primary and the November election. The Division of Elections is programming its equipment for those elections and doing other work that has to meet specific pre-election deadlines. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well. To add in a huge, expensive job requiring complicated logistics at this point is not feasible. But we recommend that it be done as soon as possible after the election.

- ***Establish security goals and a method for regularly measuring progress toward those goals.*** The Division of Elections is well aware of security issues, and has taken a number of steps to improve security. But it currently has no long-range security goals nor a plan for measuring progress. We believe it's very important for the division to develop such goals and systematically meet them.

- ***Consider forming a partnership with some other organization that could continuously monitor and evaluate*** any new election-security vulnerabilities and ways to improve security. This would allow the Division of Elections to quickly make any necessary changes or improvements, before problems developed. Some states are already doing this. The Division of Elections itself does not have adequate staff to do such monitoring.

- ***Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines***. Election officials are in fact already installing this new software, as they do programming for the upcoming election. This new software, called Key Card Tool, allows them for the first time to create their own authentication password and encryption keys for the state's 439 touch-screen machines. This is a substantial improvement in security. Previously, the default password and keys were in the public domain. They were programmed into all the touch-screen machines and couldn't be changed. Now, the password and keys can be changed regularly, and over time election regions could have their own individual passwords and keys.

- ***Verify the accuracy of voting technology.*** Before and after the November election, election officials should test all voting machines by comparing code in the machines with correct, registered code. In the longer-term, the state should develop standard testing processes to insure all voting technology is functioning properly and recording votes accurately.

- ***Change system passwords***. Before the election, the state should change all passwords currently used in election-system technology. After the election, the state should develop a plan for routinely tracking and changing passwords.

- ***Use tamper-evident seals on envelopes and shipping containers.*** This precaution can be taken before the upcoming election. Critics argue that attackers could in fact open such seals without leaving any evidence of tampering. But we believe that especially in Alaska—where ballots and equipment can travel long distances under difficult conditions—tamper-evident seals do help improve security.

- ***Recruit more poll workers and improve their election-security training.*** Before the election, the Division of Elections should add a section on election-security to the existing training manual, which doesn't currently discuss security. In the longer term, the state needs to recruit more poll workers—which in itself would help improve security in polling places—and to provide better training (possibly online) in election-security procedures.

- ***Improve the way voting machines are transported, tracked, and stored.*** Most of these recommended improvements can't be made until after the November election. They include buying better shipping containers for optical-scan machines, which have to be shipped to many small communities from larger regional centers before and elections and returned afterward. The state also needs a better system for tracking the number and location of voting machines, through bar-codes or other methods of inventory-control. Also, the physical security of machines in storage needs improvement. The state should consider reinforced doors, dead-bolt locks, ceiling grids, alarms, and other measures as appropriate.

Conclusions

We have made a number of recommendations for improving the security of Alaska's election system, but we want to keep those recommendations in context: Alaska's election system is in good shape. Other states are now adopting measures we've had in place for years. Personnel of the Division of Elections understand the system and have a good idea of what kinds of measures could help make it more secure.

But there's always room for improvement. Aside from the specific recommendations we've listed, Alaska needs to build a foundation for the future—to make sure Alaska's election system stays among the best in the country. The current election technology is aging, and the state will face new choices when it has to upgrade that technology. It needs to start systematically assessing its future needs and new technologies now.

This publication summarizes Phase 2 of the *Alaska Election Security Report,* prepared for Lieutenant Governor Sean Parnell and the Alaska Division of Elections. Contributors are LuAnn Piccard, Mark Ayers, David B. Hoffman, Stephanie Martin, and Kenrick Mock.

Table of Contents

List of Appendices

Glossary

Acronym/Phrase	Definition
AccuVote-OS or AV-OS	Premier Election Solutions optical scanning vote tabulation machine
AccuVote-TSX or AV-TSX	Premier Election Solutions touch screen voting machine
ADA	American with Disabilities Act
Chain of Custody	People, processes and locations of equipment and that have authorized custody of election material
DOE	Alaska State Division of Elections
DRE	Direct Recording Equipment (e.g. touch screen voting machine)
EAC	Election Assistance Commission
FEC	Federal Election Commission
ITA	Independent Test Authority
HAVA	Help America Vote Act
GEMS	Premier Election Solutions Global Election Management System
Memory Cards	Removable cards formatted with election information, used in optical scanning and touch screen voting machines to tally results
Premier	Premier Election Solutions formally Diebold
SAIC	Scientific Applications International Corporation
SAIT	Security and Assurance in Information Technology Lab (Florida State University)
TTBR	California Top-to-Bottom Review (commissioned summer 2007)
VSS	Voting System Standards
VVPT	Voter Verifiable Paper Trail
VVS	Voting System Standards 2002
VVSG	Voluntary Voting Systems Guidelines of 2005

Study Team

The analysis was conducted by a cross-organizational team from UAA and industry.

Principal Investigator
LuAnn Piccard, PMP, Instructor, Engineering, Science, and Project Management Department, School of Engineering, University of Alaska Anchorage

Cross-Organizational Team
Mark Ayers, P.E., Consultant, and Adjunct Faculty Member, University of Alaska Anchorage

Dr. David B. Hoffman, Adjunct Faculty and Consultant, University of Alaska Anchorage; retired Professor of Business Administration, University of Alaska Fairbanks.

Dr. Stephanie Martin, Assistant Professor, Institute of Social and Economic Research (ISER), University of Alaska Anchorage.

Dr. Kenrick Mock, Associate Professor of Computer Science, College of Arts and Sciences, University of Alaska Anchorage

Patricia Deroche, Research Associate, Institute of Social and Economic Research, University of Alaska Anchorage.

Mary Killorin, Research Associate, Institute of Social and Economic Research, University of Alaska Anchorage

Acknowledgements

The study team gratefully acknowledges help from many people.

Alaska Division of Elections
Division of Elections Director's Office

- Gail Fenumiai, State Director
- Shelly Growden, HAVA Election Systems Manager
- Jonathan O'Quinn, Election Program Manager

Region 1 Office (Juneau):

- Alyce Houston, Region 1 Election Supervisor

Region 2 Office (Anchorage, Mat-Su):

- Denali Elmore, Region 2 Election Supervisor
- Carol Thompson, Absentee and Petition Manager

Region 3 Office (Fairbanks):

- Shelly Growden, prior Region 3 Election Supervisor

Division 4 (Nome):

- Becka Baker, Region 4 Election Supervisor

Premier Election Solutions

- Kathy Rogers
- Don Vopalensky
- Ian Piper
- Dana LaTour

University of Alaska

- Fran Ulmer, Chancellor, University of Alaska Anchorage
- Diane McLean, Director Intellectual Property and Licensing

Interviewees from Alaska Cities and Boroughs

- Sherry Biggs, CMC, Borough Clerk, Kenai Peninsula Borough
- Johni Blankenship, CMC, Deputy Clerk, Kenai Peninsula Borough
- Laurie Sica, CMC, Municipal Clerk, City and Borough of Juneau
- Mona Lisa Drexler, CMC, Municipal Clerk, Fairbanks North Star Borough
- Julie Cozzi, CMC, Borough Clerk, Haines
- Harriett Edwards, CMC, Borough Clerk, Ketchikan Gateway Borough
- Colleen Pellett, CMC, Municipal Clerk, City and Borough of Sitka
- Cathy Bremner, Borough Clerk, City and Borough of Yakutat
- Tina Anderson, Borough Clerk, Aleutians East Borough
- Sheila Burke, Borough Clerk, North Slope Borough
- Tina Anderson, Borough Clerk, Aleutians East Borough
- Kate Conley, Borough Clerk, Lake and Peninsula Borough
- Carol L. Freas, City Clerk, City of Kenai
- Barbara Gruenstein, Municipal Clerk, Municipality of Anchorage
- Marjorie Harris, CMC, City Clerk, Municipality of Skagway
- Helena Hildreth, Borough Clerk, Northwest Arctic Borough

- Nova Javier, CMC, Borough Clerk, Kodiak Island Borough
- Lonnie McKechnie, CMC, Borough Clerk, Matanuska-Susitna Borough
- Gail Pieknik, Borough Clerk, Denali Borough

Interviewees outside Alaska

- Debra Bowen, Secretary of State and Lowell Finley, Deputy Secretary of State, California
- Stephen Weir, County Clerk, Contra Costa County, California
- Michael Barnes, Assistant Director, Kennesaw State University, Georgia
- Orville Brewster (Bud) Fitch II, Deputy Attorney General, State of New Hampshire

Introduction

This report details our work in Phase 2 of the Alaska Election Security study. In this phase, we developed recommendations for improving the security of Alaska's election system—not only the technology, but also the election policies and procedures. That's different from most election-security studies done in other states, which mainly assessed the security of election technology. It is electronic technology that has received the most attention in national debates about election security, but the policies and procedures—and the people who carry them out—are critical parts of any secure system.

In September 2007, Alaska's lieutenant governor, Sean Parnell, and the Alaska Division of Elections commissioned the University of Alaska Anchorage to evaluate Alaska's election systems and processes to identify security issues that could jeopardize election results. The study is in several phases and will be completed before the November 2008 presidential election. It also comes at a particularly appropriate time, since this year marks the tenth anniversary of Alaska's adoption of electronic voting technology.

The lieutenant governor—who oversees the election process—and the Division of Elections were concerned about election-security issues raised in studies done in several states. They wanted an evaluation of Alaska's election system, to identify potential security issues and measures to improve security. The Division of Elections itself first identified a number of possible security improvements, and we evaluated their feasibility and potential benefits. We also identified additional measures to enhance security.

We want to emphasize at the outset that Alaska's election system is among the most secure in the country. As we reported in Phase 1 of this study, Alaska's system includes a number of safeguards that other states are now adopting. But there is room for improvement in the technology Alaska and many other states use to count and record votes. Also, Alaska faces security issues most other states don't have. The state is huge—375 million acres—and the road system covers only about 10% of the land area. More than a hundred small, remote communities can be reached only by water or air. Storms and intense cold frequently disrupt travel and shipments to remote places. So sending ballots and election equipment to and from communities around the state, as well as storing equipment in small communities with limited facilities, is very expensive and poses many logistical challenges.

The Phase 1 report, completed in December 2007, included an overview of Alaska's voting system and discussed how our system compares with that in other states. It also summarized the findings from detailed election-security studies conducted by other states that use voting technology the same or similar to that used in Alaska. Those studies found that the current technology was potentially vulnerable to vote-tampering in a number of ways. The report concluded with a description of areas that required more detailed evaluation in Phase 2. Before we talk about our methods and findings, we first briefly discuss why election-security is an issue nationwide and describe Alaska's election system.

Why Study Election Security?

Almost all American voters now typically use some type of electronic voting equipment when they go to the polls—for instance, optical scanners that scan paper ballots and count votes, or touch-screen machines that may or may not provide any paper record of the vote. This technology has many advantages, including much faster vote-counting. Federal law also requires that all polling places have at least one machine for voters with disabilities that make it hard or impossible for them to mark paper ballots.

But many Americans are worried that these machines aren't secure—that they are vulnerable to tampering that could change the outcome of elections. The public must feel confident that every vote will be counted, and counted accurately. A number of states have examined how vulnerable voting equipment is to tampering—and found that in fact it is vulnerable in a number of ways. As we get closer to the 2008 national election, several other states and individual Americans have raised additional concerns. As a result of election-security studies and widespread publicity about security issues, some states are making changes—for example, insuring that there are paper records of votes cast electronically.

This Election Security Project has two important objectives: to help ensure the security of votes Alaskans cast and to enhance voters' confidence in the Alaska election system. That second objective is as important as the first. It's not enough to make the system more secure if Alaskans still have doubts about it. Election security should be real, both in the protections built into the system and in the minds of Alaskans—who rely on that system to count and report their votes accurately and at the same time to preserve the secrecy of the individual ballot.

It's not a simple task to build a system that provides security, accuracy, and privacy. Too much or too little focus in any single area can compromise the whole system. For example, some people have suggested that voters who use electronic voting machines could be given "receipts" that record their votes, as a demonstration of the accuracy of the system. But such receipts would not only violate the privacy of voters, they could also be used fraudulently in vote-buying schemes, in which voters would be paid for their votes after they demonstrated that they voted in a particular way.

What About Alaska?

Alaska's voting machines and other technology are manufactured by Premier Election Solutions, and are similar to equipment used in many states. The technology includes optical-scanners that scan and count votes cast on paper ballots; touch-screen machines with internal paper reels that record the votes cast; and computer servers that integrate and tally the votes. Almost all Alaska voters (99%) mark their choices on paper ballots; about 1% use touch-screen machines with internal paper reels.

Another critical part of the election system is the processes and procedures. We learned in Phase 1 that the election system includes a number of procedures that enhance security. The Phase 1 report includes a complete description of those security features, but below we summarize them briefly.

- *A single voting system, with standardized procedures and identical hardware and software, throughout the state*. This centralization of Alaska's system means that it is less complex, and it is simpler to evaluate and implement technology and procedures

statewide. Few other states have such centralized systems. For many reasons—including geography, population, history, and other factors—many states have more decentralized systems where counties, cities, or townships can make their own decisions about equipment, processes, and procedures. There is no single "right" system for all states, but Alaska's centralized approach has many benefits for election security.

- *Paper records of all votes casts*. As we noted above, almost all Alaska voters use paper ballots, and for the 1% who use touch-screen machines, there is an internal paper record. Many states have become increasingly aware of the importance of having paper back-ups. The map below, based on information from the Pew Center for the States, shows how many states have paper back-ups for votes as of early 2008. Keep in mind, however, that because most states have decentralized systems—that is, local jurisdictions can choose their own methods—the map illustrates the general rather than the exact situation in various states. In 35 states, all or almost all votes are back up by paper records. In some of those states, voters mark paper ballots, which are then scanned and counted by optical scanners. In other states, voters mostly use touch-screen machines with internal paper reels. But in early 2008, 14 states primarily used touch-screen machines without internal paper reels to provide back-ups. The Pew Center reports that two of those states—New Jersey and Maryland—have plans to implement paper-based systems. One state—New York—still uses the lever-voting system, but almost all counties plan to begin using systems that provide paper records in 2009. So overall the movement among states is toward systems with paper records—like the system Alaska already has in place.

- *Hand-counts of votes from a statistical sample of precincts across the state*. A state review board verifies the machine counts by hand-counting votes from a sample of precincts. If the hand-count results vary by more than 1% from the machine-counts in any particular precinct, votes from all precincts in the district will be hand-counted.

- *Bipartisan oversight of polling places*. Bipartisan committees oversee polling places, and political parties, independent candidates, and supporters or opponents of ballot initiatives can appoint observers to witness voting, vote counting, and vote audit procedures. Members of the public are also allowed to witness these activities.

- *Independent verification and cross-checking of paper ballots and preliminary electronic results*. Precincts separate ballots and electronic records and send them to both regional election offices and the Alaska Division of Elections for independent verification of results.

Approach to Phase 2

In Phase 1, we identified the elements that make for a secure election system, and grouped them into three categories: defense in depth, fortification of systems, and confidence in outcomes. We used those categories as a framework for assessing the level of risk presented by different security issues and for developing a set of high-priority recommendations. Some of those recommendations can be implemented during the 2008 election cycle and others will have to be done after the election. Here's how we define the parts of a secure system.

- Defense in depth. By that we mean a secure system should have multiple layers of protection, so that if one layer fails, others will remain in place. For one simple example of such depth, Alaska's electronic tallies of votes are backed up by paper ballots, measures are taken to keep the voting systems secure, and the electronic counts are verified through hand-counting a random sample of ballots. This example represents three layers of security, each of which would have to be breached in order to corrupt the election results. One of these elements might be subject to an attack or a mistake, but it is extremely likely that errors or problems would be caught by one of the other layers. Another example would be adding tamper-evident seals on the shipping packages, as well as on several parts on the outside and inside of the equipment. One exterior seal might be broken, possibly not intentionally but just while some equipment was being transported. However, if other internal seals remain in place after a systematic check of the equipment has been conducted, the equipment itself may still be secure. This is another example of a three-level defense in depth: external shipping container seals, external and internal equipment seals, and a systematic check of the equipment for evidence of tampering. We can think of defense in depth as a set of inter-related checks and balances that work together to enhance system security.

- Fortification of systems. Here we mean making electronic systems as secure as possible and using the latest updates, which often correct vulnerabilities found in earlier versions of the systems. This category also includes safeguards that ensure only authorized personnel have access to the system and that this access is properly controlled. Also, Alaska's unique conditions have security implications—for instance, voting machines are subject to temperature and transportation extremes not found in many other locations. And by law, systems used in Alaska must conform to the 2002 Voting System Standards (VSS). This equipment certification must come from a recognized Independent Test Authority (ITA).

- Confidence in outcomes. This means having systems and results that can be verified and shown to be reliable and that therefore earn the public's trust. Given the widespread distrust of electronic voting systems, this is critical. One way of building trust is being open about the system—letting voters and interested parties observe and participate in the process. Another way is keeping people informed about problems that have been identified and solutions being implemented to correct them. The intent is to correct as many issues as possible. However, in some cases after an evaluation of the costs and benefits, a decision might be made

not to correct certain issues that have a low potential for occurrence and that wouldn't have much effect if they did occur.

Multi-Phase Project

We're carrying out this project in several phases, each timed to coordinate with critical milestones in the 2008 election cycle. In Phase 1, we studied the work conducted by other states, determined its applicability to Alaska, and recommended areas for more detailed evaluation. In Phase 2, we conducted this more detailed analysis and are making detailed recommendations for consideration by the Division of Elections, for implementation in this election cycle and later. Phase 3, as determined by the Division of Elections, will provide assistance in implementing key recommendations, and Phase 4 could be a real-time system and procedural audit to verify the results of the recommendations that have been implemented. A potential Phase 5 might involve future work with the Division of Elections in the off-election cycle.

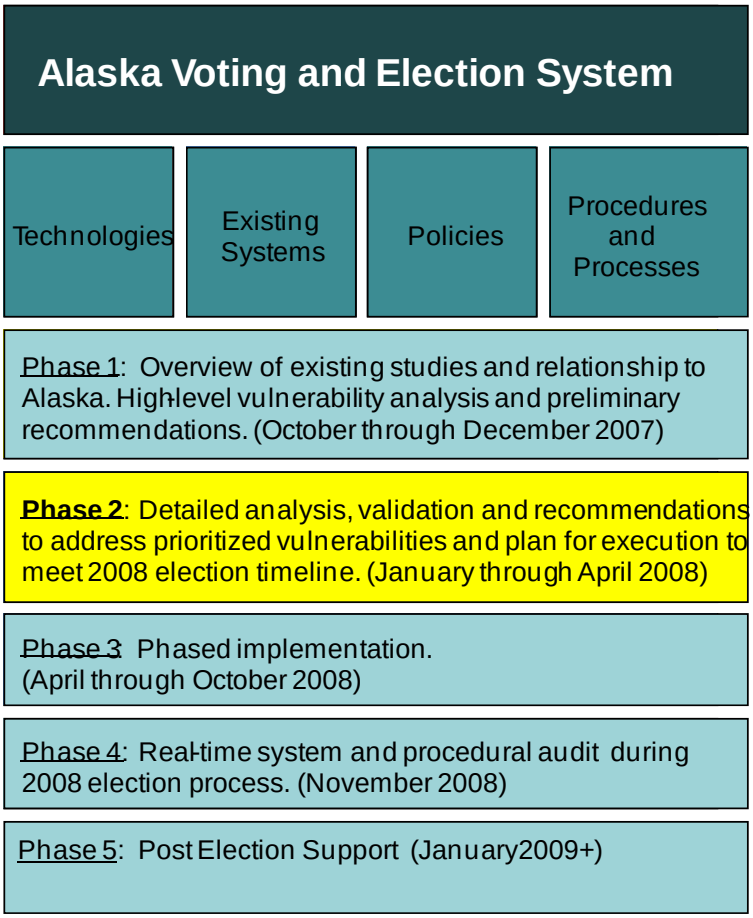


Figure 2.0 Multi-Phase Project

Scope of Work for Phase 2

The scope of work listed below summarizes the items that were selected for detailed study, grouped into the categories of defense in depth, fortification of systems, and confidence in outcomes.

Purpose: Detailed analysis of equipment and procedures and prioritized recommendations to improve Alaska election security.

1. Defense in Depth

1.1. Evaluate the cost and process to upgrade existing Premier system software and firmware if newer versions are available and certified in time to prepare for the 2008 election cycle. This analysis will be completed regardless of whether the software revisions are certified in time to implement the upgrades during the 2008 election cycle. Evaluate existing service and maintenance agreements with Premier.

1.2. Evaluate the upgraded Premier system software and firmware changes that have been submitted to the EAC for VSS 2002 Certification against potential and known security vulnerabilities identified in the Phase 1 report and as they relate to the security enhancements proposed by the Division of Elections. Summarize the original issue or concern and how the new version of Premier software and firmware may address (or may not address) the issues. (See attached document provided by Division of Elections for detailed list of items.)

1.3. Evaluate the existing Premier system software and firmware currently in use in Alaska. Determine if the security enhancements proposed by the Division of Elections can be implemented if current versions of tabulation software and firmware remain in use.

1.4. Provide recommendations to the Division of Elections on how existing procedures can be improved to address any identified security issues.

1.5. Evaluate password management options, recommend alternatives and propose appropriate processes and procedures.

1.6. Document inter-election chain-of-custody for voting equipment. With the knowledge that voting equipment is out of the DOE's custody during points in the election process, assess the risks of tampering, damage, and loss and provide recommendations to mitigate those risks.

1.7. With the knowledge that Alaska, for logistical purposes, stores touch screen and optical scan units off site between elections, determine best practices for storage and determine whether they would be feasible in Alaska communities. Recommend solutions that can meet security requirements and can also be practically implemented in the Alaska environment.

1.8. Identify trusted personnel within the Division of Elections and their points of access to equipment. Identify points of equipment access where only one person has access or authorization.

1.9. Determine points in election system where more redundancy in personnel, processes and /or joint review processes should be implemented.

1.10. Assess vulnerability of paper ballots to tampering. Contrast with risks in electronic system.

1.11. Summarize the security vulnerabilities of the equipment and procedures. To the extent possible, demonstrate the level to which proposed enhancements (equipment and procedures) mitigate security risks.

1.12. Develop security training procedures that can be included as an addendum to existing training documentation.

2. Fortification of Systems

2.1 Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.

2.2 Evaluate communication protocols and make recommendations regarding data transmittal to GEMS to avoid the introduction of viruses and longtime delays in election returns.

2.3. Evaluate the reliability and accuracy of the optical scanning and touch screen systems and their ability to function properly in Alaska weather and transportation/handling conditions. Study existing Premier reliability testing levels and equipment maintenance procedures to identify any concerns.

3. Confidence in Outcome

3.1 Evaluate processes and procedures DOE uses for functionality testing and logic and accuracy testing of systems and memory cards.

3.2 Identify methods DOE can use to increase voter confidence.

3.3 Establish metrics that the DOE can use to demonstrate continuous improvement of election security and predictability of results over time.

3.4 Provide a weekly review of emails from the public on security issues and summarize and publish general responses to them on Division of Elections website. Participate in other forums as requested by Division of Elections.

3.5 Provide a description of the absentee and questioned ballot process.

3.6 Research other random sampling methodologies that might provide additional confidence in election results. These recommendations would be proposed for future consideration and evaluation.

4. Evaluation and Implementation Plan

4.1 Synchronize Phase 2 work-plan with 2008 election process timeline to ensure that completion of critical evaluation deliverables and recommendations are phased with implementation deadlines as determined by the Division of Elections.

4.2 Develop project plan to implement prioritized recommendations (technology, systems and procedural) developed during Phase 2 work phased to meet 2008 election process timeline. If approved, this plan would be the basis of "Phase 3: Execution of Phased Deliverables."

Time Frame: Mid January 2008-end April 2008.
(Completion of deliverables will be phased throughout Phase 2 in accordance with section 4.1).

Cost (Est.): $250,000

Exclusions:

1. Detailed hands-on testing of the equipment in operation.
2. Destructive testing of equipment.
3. Payment for equipment, hardware, software firmware, tools, personnel, packaging, etc. required to upgrade election systems and procedures.
4. Usability analysis of touch screen systems (e.g. ease of use, language, user interface, set-up/tear-down, etc.)
5. Inventory analysis of existing equipment.
6. Documentation review and analysis.
7. Analysis of voter registration process.

Summary of Recommendations

We conducted analyses for each item on the scope of work listed above. Here we summarize the evaluation we conducted for each item of the scope of work and the relevant recommendations. More detailed information is included in the report appendixes, with the appropriate appendix cited in the summary.

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
		1.0 Defense in Depth		
1.1	Assure 1.2 Upgrade Cost Analysis	Maintain current revision of AccuVote software, perform cost benefit analysis to determine best resource utilization approach.	Upgrade to Assure 1.2 when certified	Appendix A - Assure 1.2 Upgrade Labor Estimate
1.2	Assure 1.2 Functionality Upgrade Analysis	Maintain current revision of AccuVote software.	Upgrade to Assure 1.2 when certified	Appendix B - Assure 1.2 Upgrade Analysis Appendix C - Assure 1.2 Upgrade Resolution Matrix
1.3	Division of Elections Security Enhancements and Features Analysis	Implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.18, 2.19, 2.23, 2.29	Implement remaining recommendations included in Appendix D.	Appendix D - Division of Elections Enhancement Analysis
1.4	Implement procedures to minimize technology risks not addressed by existing or upgraded systems	Implement procedures described in other sections. Important to maintain many of the processes already in place.	Monitor research on election processes and implement changes, as appropriate.	
1.5	Password Management	Change passwords on all affected hardware as outlined in password management plan (Appendix E).	Develop password management procedures to implement password changes and tracking for future election cycles to ensure password policies are followed consistently.	Appendix E - Physical Password Management Recommendations
1.6	Chain of Custody	Begin to use tamper evident seals on AV-OS and AV-TSX machines.	Further implementation of tamper evident seals. Implement EPROM bar code identification and inventory management.	Appendix G

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
		1.0 Defense in Depth (cont.)		
1.7	Best practices for equipment storage between elections	Follow Chain of Custody recommendations. Purchase Division of Elections owned equipment for North Slope Borough. Safes are recommended for use in Division of Elections offices to store keys and passwords.	Improve physical storage security such as room security, access alarm, etc.	
1.8	Trusted Personnel and single points of access	None	Require background checks on new employees with access to election equipment and confidential information	
1.9	Redundancy	Two person inspection and sign off on tamper evident seals.	Add two-person sign-off to manual entry of election results and tamper seal inspections.	
1.10	Paper Ballot tampering vulnerability	None	None	
1.11	Master Vulnerability Matrix	N/A	N/A	Appendix R - Master Matrix Recommendations, Risk and Value Assessment Appendix S - 2008 Election Cycle Impact Matrix Appendix T - Future Election Cycle Impact Matrix
1.12	Security Training	Develop materials to train poll worker in election security.	Monitor new procedures and expand training as appropriate.	Appendix H

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
2.0 Fortification of Systems				
2.1	Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.	Implement Key Card Tool application. Implement GEMS Air Gap Server model system. Implement dedicated AV-OS machine for programming AV-OS memory cards.	None	Appendix O - Security Key Card Enhancement Options Appendix P - Security Key Card System Description Appendix M - AccuVote Functional Test Guidelines
2.2	Preliminary Results Data Collection Assessment	None	None	Appendix J - AccuVote Communications System Description Appendix K - AccuVote Network Topology
2.3	Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.	None	Implement new shipping containers for optical scanning systems (PelicanTM. Products 1600 series or similar)	Appendix L - AccuVote Reliability Assessment Appendix I - AV-OS Shipping Container Example

Section	Scope of Work Item	Current Election Cycle Recommendation	Future Election Cycle Recommendation	Appendix Reference
3.0 Confidence in Outcomes				
3.1	Procedures for functionality, logic and accuracy testing for systems and memory cards.	Implement increased test scope for functional, logic and accuracy testing.	Implement test results documentation and storage policies.	Appendix M - AccuVote Functional Test Guidelines Appendix N - AccuVote Logic and Accuracy Test Guidelines
3.2	Methods to improve voter confidence	Increase voter use of AV-TSX machines to improve voter anonymity.	Monitor research on election processes and implement changes, as appropriate.	
3.3	Metrics and continuous improvement	Implement a multi-year, multi-phase approach to improving election procedures and equipment.	Multi-year, multi-phase approach	Appendix F - Chain of Custody Map
3.4	Weekly email summary	Provide on-going summary	Provide on-going summary	
3.5	Absentee and questioned ballot process	Implement 2008 election cycle security improvements.	Same as current election recommendations.	Appendix Q - Summary of Absentee Voting
3.6	Random sampling methodologies	None. Current research is not conclusive enough to recommend a change to the Division of Elections methodology.	Implement new sampling procedure as appropriate and approved by statute.	

Part 1 Defense in Depth

Section 1.1 – Premier Election Solutions Assure 1.2 Software Upgrade Cost Analysis

Description:

Evaluate the cost and process to upgrade existing Premier Election Solutions (Premier) (formerly Diebold) system software and firmware if newer versions are available and certified in time to prepare for 2008 election cycle. This analysis will be completed independently of whether the software revisions are certified in time to implement the upgrades during the 2008 election cycle. Evaluate existing service and maintenance agreements with Premier.

Summary of Analysis:

The cost to upgrade from the existing AccuVote software and firmware revisions consists of contributions from two different upgrade components.

The first component is the cost to purchase the software and firmware components from Premier. The Division of Elections has a current maintenance agreement with Premier which includes software and firmware upgrades at no additional cost.

Implementation of the Assure 1.2 upgrade requires software and firmware upgrades to be performed on all major AccuVote system components. The labor estimate table provided in Appendix A – Assure 1.2 Upgrade Labor Estimate provides a list of the tasks required to be completed for the Assure 1.2 upgrade as well as an estimate of 995 person-hours to implement a system-wide firmware/software upgrade AV-OS, and AV-TSX. Labor associated with each upgrade task is provided as estimated hours. Actual hours were not measured for the purposes of this report. The comprehensive nature of the Assure 1.2 upgrade requires that a complete acceptance test be performed following the upgrade to ensure system functionality and reliability.

Recommendation:

2008 Election Cycle

We recommend that the Division of Elections do a cost benefit analysis to determine whether performing the upgrade using Division of Elections resources, external contractors or contracting with Premier is a more cost effective approach for implementing Assure 1.2.

Post Election

We recommend implementing the Assure 1.2 upgrade upon certification by the Election Assurance Commission (EAC) to the Voting Systems Standards (VSS) 2002 using the resources deemed most cost effective in the 2008 election cycle.

Section 1.2 – Premier Election Solutions Assure 1.2 Software Upgrade Enhancement Evaluation

Description:

Evaluate the upgraded Premier system software and firmware changes that have been submitted to the federal EAC for VSS 2002 certification against potential and known security vulnerabilities identified in the Phase 1 report and as they relate to the security enhancements proposed by the Division of Elections. Summarize the original issue or concern and how the new version of Premier software and firmware may address (or may not address) the issues.

Summary of Analysis:

Phase 1 of the State of Alaska Election Security Project (SOAESP) examined the current body of knowledge surrounding the Premier AccuVote voting system platform. This examination was focused on identifying areas of vulnerability within the AccuVote system currently in use by the Division of Elections. Phase 1 of the SOAESP reported that research conducted by the states of California (Calandrino, et al., 2007; Bishop, 2007), Florida (Gardner, et al., 2007) and others found vulnerabilities in the AccuVote platform currently in use by the Division of Elections as well as many other states. Premier responded to this research by producing revised versions of the software and firmware that operate on various components of the AccuVote system and address a number of the identified vulnerabilities.

An examination of the AccuVote software, firmware and hardware components used by the Division of Elections as well as an analysis of the vulnerabilities identified by the states of California, Florida and Alaska are provided in Appendix B - Assure 1.2 Upgrade Analysis. This appendix provides a summary description of each vulnerability or issue identified by California, Florida or Alaska. The status of each vulnerability is provided in tabular format in Appendix C – Assure 1.2 Upgrade Resolution Matrix.

A total of 38 individual vulnerabilities, issues or risks are identified and itemized for evaluation against the Assure 1.2 revision. These items are compared with the Assure 1.2 functionality to determine whether the vulnerability, issue or risk remains following the installation of the Assure 1.2 software or firmware. Installation of the Assure 1.2 revision reduces the number of vulnerabilities, issues and risks to 13.

By Alaska statute, the Assure 1.2 AccuVote revision must comply with VSS 2002 before it can be used in Alaska. Certification by an approved Independent Test Authority (ITA) is required to verify compliance to the VSS 2002 standard. At the time this document was written, the Assure 1.2 revision was under test by SysTest, an approved ITA, and certification had not yet been granted.

Recommendations:

The Assure 1.2 AccuVote revision includes significant improvements in overall system security performance. The system revision provides patches to public domain bugs, known vulnerabilities and system use issues.

2008 Election Cycle:

We do not recommend implementation of the Assure 1.2 upgrade during the 2008 election cycle. Since the Assure 1.2 revision has not yet been certified to the VSS 2002 standard, we cannot recommend that it be implemented prior to the 2008 election year primary and general elections. Furthermore, even if the software were to become certified prior to the elections there is insufficient time and resources to implement the revision before election programming must begin.

Post Election:

We recommend that the Assure 1.2 AccuVote revision be installed following the 2008 election cycle and once the appropriate VSS 2002 certification has been obtained.

Section 1.3 – State of Alaska Division of Elections Proposed Enhancement Evaluation

Description:

Evaluate the existing Premier system software and firmware currently in use in Alaska. Determine if the security enhancements proposed by the Division of Elections can be implemented if current versions of tabulation software remain in use.

Summary of Analysis:

The State of Alaska, Division of Elections has produced an internal document, *AccuVote Security Enhancements and Features* (2007). This document is a list of internally recommended security enhancements identified by the Division of Elections. A request was made of the project team to evaluate whether any or all of the proposed enhancements could be adopted within the structure of the currently operated AccuVote software, firmware and hardware platforms.

All of the recommended enhancements can be implemented on the current system with little to no impact on system performance. Implementation of the feature and enhancement list is limited by Division of Elections resource availability.

A detailed discussion of each feature or enhancement is provided in Appendix D – Division of Elections Enhancement Analysis. A cross-reference between the Division of Elections AccuVote Security Enhancements and Features and Appendix D – Division of Elections Enhancement Analysis is provided below.

Division of Elections Heading	Appendix D Section
GEMS Software and Computers	Sections 2.1 to 2.7
Memory Cards	Sections 2.8 to 2.16
Voting Equipment	Sections 2.17 to 2.25
Testing and Audits	Sections 2.26 to 2.28
Administrator Card	Section 2.29
City/Borough	Sections 2.30 to 2.31

Recommendations:

2008 Election Cycle:

We recommend that the Division of Elections implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. A subset of the recommendations in Appendix D (Sections 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.17, 2.18, 2.19, 2.23, and 2.29) should be adopted during the 2008 election cycle. Highest priority should

be placed on hash validation, access control and password management, chain of custody assurance, and tamper evident security measures.

Post Election:

The balance of the enhancements not performed during the 2008 election cycle can be implemented between the 2008 and 2010 election cycles. This phased implementation approach will address the most critical issues first and provide an opportunity for the Division of Elections to balance multiple resource demands during this election year.

Section 1.4 – Procedural Security Enhancements

Description:

Provide recommendations for improving existing procedures to address security issues.

Recommendations:

2008 Election Cycle

Many of the Division of Elections' existing procedures work well and need to be maintained. Among these are post election precinct level reconciliation, post election audit, election officials as state employees (rather than political appointees), use of chain of custody, current ballot printing company, allowing/encouraging observers.

We recommend using tamper evident seals on election equipment (Section 1.7) and having poll workers inspect seals (Section 1.12), increasing poll worker awareness of tampering risks (Sections 1.6 and 1.12), implementing background checks for employees with access to sensitive information and voting equipment (Section 1.8), requiring two people to sign off on many procedures (Section 1.9), and ensuring that when voters use AV-TSX machines, at least five people vote on them (Section 3.2).

Post Election

Continue to monitor research on election processes and procedures. Make changes to Alaska's system as appropriate.

Section 1.5 – State of Alaska Division of Elections Password Management Options Evaluation

Description:

Evaluate password management options, recommend alternatives and propose appropriate processes and procedures.

Summary of Analysis:

The Division of Elections has a desire to improve its handling of passwords. The division manages several sets of security controls accessed by password to implement an election. These security controls consist of physical security, computer Built-in Operating System (BIOS) security, Windows operating system login security and Global Election Management System (GEMS) database security. These domains form a hierarchical password security system in which multiple levels of security penetration are required to gain access.

Physical security and access to servers and voting machines was found to be inconsistent across voting regions with some regions executing physical security in a more robust manner than other regions. The Division of Elections does not currently implement BIOS passwords on any of the GEMS servers in the AccuVote system. Additionally, although the Division of Elections currently uses a password management plan for its Windows login and GEMS database, room for improvement exists in the management of passwords for both of these security domains.

Appendix E – Physical Password Management Recommendations reviews the current Division of Elections password management policies and makes a series of recommendations regarding each of the security domains.

Recommendations:

2008 Election Cycle:

We recommend changing passwords on all hardware and software platforms as outlined in Appendix E – Physical Password Management Recommendations. Development of formal policies to accompany the password changes during the 2008 election cycle is not recommended due to resource constraints.

Post Election:

We recommend that the Division of Elections make improvements to the consistency and fortification of physical security access at equipment storage locations as well as implement structured password management policies for each password security domain within the AccuVote system. The structured password management policies should

include documentation guidelines and formal procedures associated with the implementation of the password management plan. A more detailed description of these recommendations is provided in Appendix E – Physical Password Management Recommendations.

Section 1.6 - Chain of Custody

Description:

Document the inter-election chain-of-custody for voting equipment. With the knowledge that voting equipment is out of the Division of Election's custody during points in the election process, assess the risks of tampering, damage, and loss and provide recommendations to mitigate those risks.

Summary of analysis:

We define "chain of custody" to mean traceability of secure storage and transportation of election equipment during all phases of an election cycle and in between election cycles. Election equipment includes: ballots, AccuVote optical scan (AV-OS), AccuVote Touch Screen (AV-TSX) machines, and memory cards. An overview of Alaska's chain of custody procedures for road connected communities and map of Alaska's chain of custody is included in Appendix F - Chain of Custody Map.

The chain of custody works well for sending election equipment among Alaska's larger and road connected communities. However, 41% of the state's precincts (179 out of 439) are off the road system and can only be reached by boat or airplane[1]. This represents about 17% of voters (77,000). As a result, chain of custody documentation is not feasible and secure storage space for election equipment may not be available. These conditions cause some of the election machines to be vulnerable to tampering during transit and storage. Additionally, many of the AV-TSX and AV-OS machines remain in communities between the primary election in August and general election in November[2]. Some municipalities and boroughs use the AV-OS machines in municipal elections in October. The AV-OS machines are outside of the state's chain of custody when used in municipal elections.

Prior to the primary election, OS machines are stored in regional centers, satellite offices or hubs. Several weeks before the primary election, the regional offices test AV-OS machines with their memory cards inserted. Memory cards are sealed inside the AV-OS machines and they are sent out to AccuVote coordinators in communities. Following elections, some machines are stored in communities, others are returned for storage in hubs or regions. Storage is less centralized between the primary and general election than prior to the primary. Memory cards are sent to AccuVote coordinators in communities where AV-OS machines have been stored. For the general election machines are again tested with their memory cards.

---

[1] Some have ice road access in the winter.

[2] Shipping AV-TSX machines back to regional hubs would double the shipping costs, and require more election staff. It is a logistical challenge to send AV-TSX machines (weighing 60 pounds), ballots (another 25 pounds), printers, voting booths, and ballot boxes by small air carrier to hundreds of remote communities.

Because of time and staffing constraints, AV-TSX memory cards are currently batch tested and inserted into machines on election day. The alternative would be to test each memory card in its AV-TSX machine, seal the card and ship the machines with cards inserted to precincts for primary elections, then ship all machines back to hubs or regional centers and repeat the process prior to the general elections. It is not feasible to ship all machines back to regional hubs and back out to precincts between elections. It would double the current transportation costs and more than double staff time. After the primary, Division of Elections staff members are busy preparing for the general election. To set up and test each AV-TSX machine with a memory card inside would take 30 minutes per machine. We estimate that it would take a minimum of 220 hours (about 5.5 weeks) to test machines one-by-one.

The North Slope Borough owns several AV-OS machines. In past state/federal elections the state borrowed AV-OS machines from the borough. The borough's machines are outside of the state's chain of custody and security domain. The state has addressed this problem by purchasing additional state-owned AV-OS machines to use in North Slope communities.

Recommendations:

2008 Election Cycle:

We recommend continuing to use the current system for shipping and testing AV-OS machines and their memory cards.

We recommend Division of Elections continues to ship AV-TSX memory cards separately from machines.

We recommend using tamper evident seals[3] on all AV-OS and AV-TSX machines. In collaboration with California counties, Premier developed best practices for use of tamper evident seals (Premier Election Solutions 2008). Appendix G - Premier Best Practices for Tamper Evident Seal Placement contains the Premier document. Although Premier recommends using two seals[4] on AV-OS machines and three seals on AV-TSX machines, we recommend that the Division of Elections adopt a phased approach to using tamper-evident seals. Because election equipment is shipped around the state and may be subjected to rough handling and harsh weather conditions, we recommend using one seal on each AV-OS and each AV-TSX machine in 2008. If there few false alarms and as seal inspection and reporting methods are fine tuned, we recommend increasing the number of seals per machine in future election cycles.

[3] We take into consideration the finding in California's top-to-bottom review that tamper evident seals are easy to remove and replace (Calandrino et al. 2007). We see implementing tamper-evident seals as a way to make attacks more difficult or riskier, but not necessarily impossible (Johnston 2006).
[4] Intab and Seton corporations manufacture seals used successfully in Premier tests

For AV-OS machines a serialized tamper evident security seal should cover either the front "seam" or the back "seam" and screw hole. Refer to Appendix G for Premier's illustrated documentation of security seal placement.

For AV-TSX machines; following Premier's recommendations, the seal should cover the "seam" and a screw hole on the back of the machine. (See pictures in Appendix G)

Memory cards: For locations where AV-TSX machines are stored between primary and general elections, we recommend mailing AV-TSX memory cards in tamper-evident envelopes or bankers bags.

In addition to using tamper-evident seals, we recommend providing poll workers with a check list and procedures for seal inspection and instructions for what to do if seals are broken. (See Appendix H - Security Training).

The regional office in Fairbanks currently uses a Microsoft Excel based inventory management system. We recommend using this system state-wide.

Post Election:

If using one tamper-evident seal on each machine is successful, we recommend expanding the use of tamper-evident seals in accordance with Premier's best practices. AV-OS machines: in addition to the seal over the front or back seam, the memory card slot should be sealed with serialized security seal. Refer to Appendix G for Premier's illustrated documentation of security seal placement.

AV-TSX machines: In addition to the seal over the seam, we recommend two additional tamper-evident seals on each AV-TSX unit. One of the seals should cover the memory card slot. The second seal should seal the privacy panels that cover the touch screen panel (See pictures in Appendix G). We also recommend using tamper-evident serialized seals on the metal shipping cases.

We recommend implementing a bar code system to keep track of equipment.

Section 1.7 - Storage of Election Equipment and Material

Description:

With the knowledge that Alaska, for logistical purposes, stores touch screen and optical scan unites off-site between elections, determine best practices for storage and determine whether they would be feasible in Alaska communities. Recommend solutions that can meet security requirements and can also be practically implemented in the Alaska environment.

Summary of analysis:

This refers to the physical storage of election equipment: ballots, memory cards, GEMS servers, and peripherals AV-OS and AV-TSX machines. We evaluate storage practices in Alaska given the logistical challenges and make recommendations that take them into account.

We visited and examined storage sites in Anchorage, Fairbanks, Juneau and Kenai and interviewed the regional director in Nome, Juneau and Fairbanks, all borough clerks, several municipal clerks. We also reviewed Premier/Diebold recommendations and other documents. Uniform practices for storing election machinery would be ideal, but differences in building construction and lease arrangements limit the ability of Division of Elections to implement a completely uniform storage practice. Storing AV-OS and AV-TSX machines in remote communities prior to and between elections complicates equipment storage.

Recommendations:

2008 Election Cycle

Regional and state storage areas should have a safe in the director's office for storage of keys and password codes.

We recognize that AV-TSX machines are big and take up a lot of storage space. If possible, in remote communities, equipment should be stored in a lockable closet within a municipal or tribal office. If such a facility is not available, machines should be stored in a facility that can be locked when the person responsible for the equipment is not present. Poll workers' training needs to emphasize the importance of secure storage.

For equipment in non-secure facilities, additional precautions including inspections, and functional tests should be conducted in advance of equipment use to ensure that any tampering or reliability issues can be proactively identified. (See Appendix H-Security Training.)

Post Election

- A monitored alarm system in all secure storage rooms
- Deadbolt locks on secure storage room doors
- Self-closing/locking doors
- Metal ceiling grids in locations where walls do not extend to the roof or upper floor structure.
- Keyless entry for secure storage rooms with automatic logging of entry and exit.
- Motion detection security cameras.
- For the state GEMS storage room in Juneau, we recommend relocating network switching equipment outside of the election equipment room.

The Division of Elections officials should consider the ease in securely storing and shipping equipment in their decisions about future equipment purchases.

Section 1.8 – Trusted Personnel and Single Points of Access

Description:

Identify trusted personnel within the Division of Elections and their points of access to the equipment. Identify points of equipment access where only one person has access or authorization.

Summary of analysis:

We interviewed Division of Elections staff to identify places in the system where a single person has access to software, machines, or election material. We found several instances of singular access. The GEMS programmer in Juneau, AccuVote coordinators, poll workers who store election equipment, and pilots and air carriers who transport machines all represent positions in the election system with singular access to election components. The GEMS database is a Jet database file (similar to Microsoft Access). Programming the election involves filling in fields in the interface. The GEMS program has built-in checks for errors and prompts the user to make changes. Several people besides the programmer review ballots before they are sent to the printer[5]. The Division of Elections has a small staff, some of whom have been at their jobs for almost 20 years. The system relies on a high degree of implied trust. Tampering with electronic results could be detected by the random audit conducted as part of every election.

Recommendations:

2008 Election Cycle:

We recommend continuing to use one person to enter elections information into GEMS. Having multiple people programming the elections database is problematic. Alaska's boroughs and municipalities that use GEMS and Kennesaw State University Election Center (which programs ballots for the state of Georgia) use one person to enter elections information into GEMS. The use of a single person is believed to result in fewer errors because one person is keeping track of changes to the system. The enhanced logic, accuracy, and integrity testing procedures increase the probability of detection of errors and issues with election programming prior to deployment for use.

Post Election:

For the positions of election programmer, regional director, and absentee director we recommend implementing a program of background checks for new hires, in accordance

[5] Boroughs and municipalities in Alaska use a similar system of proof-reading. Georgia loads a test ballot into the AV-TSX machine as part of the proof reading (however, over 99% of voters there use touch screen devices).

with state law and labor union agreements. We recommend that the Division of Elections recruit and train more AccuVote coordinators.

Section 1.9 – Redundancy

Description:

Determine points in election system where more redundancy in personnel, processes, and/or joint review processes should be implemented.

Summary of analysis:

Redundancy can not only protect the election system from tampering, it can also lower the chance of errors[6]. In election systems there is a trade-off between the proprietary nature of the election information and having staff redundancy to safeguard the system. Division of Elections has several people trained in GEMS programming, in addition, several borough level officials are also trained in GEMS programming. Elections could proceed if the primary programmer was unavailable due to extenuating circumstances. The state has seven people with access to GEMS: one with programming access, six with access at regional offices. The state requires two elections officials or poll workers present during logic and accuracy testing, and equipment packing for shipment to precincts. Joint review for some polling place tasks[7] is difficult in practice.

Recommendations:

2008 Election Cycle

Maintain current two-person sign-off on precinct level post-election practices of checking vote tallies and registration lists and reporting results.

Add second person or have cross-checking review for the following tasks:

- Verification of tamper-evident seal integrity.
- Verification of tamper-evident seal serial numbers.
- Manual entry of election results into GEMS.

Post Election:

Increase focus on poll worker recruitment.

---

[6] Despite all the attention devoted to potential tampering, researchers found that past problems with election results were due to human error or equipment problems, and not malicious intruders (Thompson 2008, Herrnson et al. 2008).

[7] Alaska's instructions for AV-TSX setting up recommend that one person read instructions, another set up the machine. Two people are also required to sign off on zero totals on AV-OS and AV-TSX tallies. People are also required to set up tables, post signs, assemble voting booths, and organize registration books and other voting materials. Sometimes all task need to be done within 30 minutes, by poll workers whose average age is 72. If a polling place is short staffed, its unlikely two people will be available for tasks.

Section 1.10 – Paper Ballot Tampering Vulnerability

Description:

Assess vulnerability of paper ballots to tampering. Contrast with risks in electronic system.

Summary of analysis:

Paper ballot tampering is easier to detect than electronic tampering because it takes more people, better organization, and a higher level of secrecy to tamper. (Norden, et al. 2007). Changing election results on a large scale by tampering with paper ballots scale requires widespread access.

Ballot stuffing is a one way to tamper with paper ballots. However, Norden et al. (2007) write that it would take several election insiders at each polling place to carry out a ballot stuffing attack. Insiders need to steal ballots, copy and mark them, insert extra ballots into the optical scanner or ballot box, and adjust voter registration books. Despite this potential attack scenario, the polling place post-election accounting process (comparing number of ballots cast with number of signatures in the registration book) would likely detect a ballot stuffing attack. A second process check at during the statewide audit of post-election results could also detect ballot stuffing.

Vote buying is another method of tampering with paper ballots. A vote buying scheme would involve hundreds of people and would require that hundreds of people keep quiet. People would also need to be able to demonstrate that they voted as instructed. Voter secrecy helps guard against vote buying schemes by prohibiting issuance of a vote receipt. According to Shamos (2004) vote receipts could create an epidemic of vote-buying.

Paper ballots can be also be damaged or lost during transit. Maintaining electronic vote records can mitigate the impact of this risk. Secure ballot provides additional safeguards. In Alaska, by law, if ballots are lost, the state can mandate a new election.

Ballot printing mistakes can disrupt an election. Ballots need to be printed and cut according to strict equipment vendor specifications so that they can be fed smoothly into the AV-OS machines and read accurately without jamming. Ballot printing is a specialized process. Mistakes could prevent accurate ballot insertion and vote counting, perhaps on a state-wide level. To date, there have been no reported issues relating to the physical attributes of the ballots from the current ballot printer. The current ballot printer used by the state has proved to be reliable and accurate. For their elections, most boroughs and municipalities also contract with the same ballot printer[8] that Division of Elections uses.

[8] Boroughs that don't use Print Works send their ballots out-of-state to Premier to print their ballots.

Recommendations:

2008 Election Cycle:

Maintain current relationship with Print Works in Homer. There are not a lot of people in the country who can consistently and accurately produce ballots that comply with the AccuVote system. Ballot printers for ballots used with AV-OS systems must be certified to Premier standards. The recent move of many states to paper ballots is pushing the capacity of the current printing infrastructure.

Post Election:

This system works very well at present. However, since there is not another qualified in-state ballot printer alternative, it would be beneficial to identify a qualified back-up.

Section 1.11 – Security Vulnerability Matrix

Description:

Summarize the security vulnerabilities of the equipment and procedures. To the extent possible, demonstrate the level to which proposed enhancements (equipment and procedures) mitigate security risks.

Summary of Analysis:

The intent of the security vulnerability matrix is to convey the major findings of Phase 2 in a clear, concise manner. The matrix presents the findings in terms of two parameters. See Appendix R - Master Matrix: Recommendations, Risk and Value Assessment.

Risk represents a qualitative estimate of the risk level associated with each item in the Phase 2 project scope. Risk is shown on a three level scale of high, moderate and low. The risk value assigned for each item is not a measureable quantity but rather an aggregation of information obtained during research conducted throughout Phase 2. High risk items are intended to identify areas where focus should be immediately applied. Moderate risk items identify areas requiring attention which should be addressed within a reasonable period of time. Low risk items offer little or incremental increase in performance.

Value represents the amount of benefit obtained by executing a recommendation. Value is rated on a scale of one (lowest) to three (highest). Items with the highest value represent good investments of labor and material resources. The benefit obtained by high value recommendations result in a reduction in component or overall system risk. Items with values of one or two represent investments which may require further research or justification. Clearly, low value, low risk items should be carefully studied before financial investment is made to ensure that implementation of the recommendation makes sense.

The matrix provides a series of columns which describe each scope item (consistent with the Phase 2 scope) and a risk associated with the current system implementation. Additional columns represent recommendation execution value and residual risk remaining following the execution of a recommendation. Resource and time constraints do not allow the Division of Elections to execute all of the suggested recommendations prior to the 2008 election cycle. As such a further set of columns represents the value and residual risk associated with implementing recommendations following the 2008 election cycle. Finally, a column is provided which provides constraints, limitations or notes associated with an individual scope item.

In addition to the matrix provided, a graphical representation of the current (2008) election cycle and the future election cycle scope items is provided. The purpose of these figures is to provide a fast, easy method to interpret the results in the matrix. A grid of 9

boxes represents the current value of risk for each scope item. Presence of a box with the scope items task number in a grid cell indicates its risk and value. The color (black, gray, white) represents the residual risk remaining if the recommendations provided are implemented

Section 1.12 – Security Training

Description:

Develop security training procedures that can be included as an addendum to existent training documentation.

Summary of analysis:

Poll workers represent one of several layers of defense in depth to help observe and guard against tampering. Currently Alaska poll worker training material does not include any security training. Not all of Alaska's poll workers attend training sessions. We reviewed and collected training documents from other election jurisdictions including California counties, Florida, Georgia, Indiana, Maryland, Mississippi, Missouri, New Hampshire, New York City, Ohio, and Wisconsin. Other research shows that better poll worker training is associated with increased voter confidence (Pew Center on the States, 2007). Weiser and Goldman (2007) recommend uniform statewide training.

Recommendations:

2008 Election Cycle:

We recommend training and checklists that will increase poll worker awareness of the possibility of attacks. Training which reminds poll workers of the importance of vigilance and secure equipment storage is part of building a multi-layer defense in depth election security system. It is also important to be alert to unusual and suspicious situations. For example, one such attack might be an attempt to divert poll workers attention to a false emergency. Another might be a disruption that could cause a massive denial of service. These kinds of disruptions are most likely in close races, in precincts where a candidate expects to lose.

We also recognize that poll workers are temporary employees and have a responsibility to not impede elections. Election crimes include causing eligible people to be excluded from elections, eligible votes not to be cast or counted, or other interference with election results (EAC 2006). It is important for poll workers to maintain the delicate balance between security and facilitating voting for all eligible voters.

We recommend training poll workers to inspect tamper evident seals.

We recommend that the Division of Elections provide more specific instructions how to "store your ballots, optical scan unit, and touch-screen voting unit in a secure location" in training (State of Alaska 2006). Refer to Appendix H - Security Training for more information.

Post Election:

Suggested changes to poll-worker training include enhanced security procedures as well as use of more effective training methods. The Division of Elections should consider implementing on-line training programs in addition to in-person training sessions. Consider certification and/or increase in poll-worker pay tied to successful completion of training. Poll worker wages are currently set by state statute so increases in wages would require legislative approval.

Part 2 Fortification of Systems

Description:

Section 2.1 Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.

Section 2.2 Evaluate communication protocols and make recommendations regarding data transmittal to GEMS to avoid the introduction of viruses and longtime delays in election returns.

Section 2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems and their ability to function properly in Alaska weather and transportation/handling conditions. Study existing Premier reliability testing levels and equipment maintenance procedures to identify any concerns

Summary of Analysis:

The AccuVote election system is made up of voting components which are physically distributed across the State of Alaska. The AV-OS and AV-TSX voting machines are used to capture and tally votes within individual precincts. Six GEMS servers are also used during an election to enter hand-counted paper ballots on election night. The AccuVote system allows the election administrators to tabulate preliminary, unofficial results rapidly by transmitting the results stored in memory cards from each AV-OS and AV-TSX machine to a GEMS server in Juneau where the preliminary results are tabulated on a statewide level.

The current election system is implemented using a single director's office GEMS server which is used for both election programming and preliminary vote tabulation on the night of the election. AV-OS memory cards are programmed in the Juneau director's office using an AV-OS machine connected to the director's office GEMS. This machine is responsible for programming all of the AV-OS memory cards for the election state-wide.

The transmission of each AV-OS and AV-TSX machine's results is performed using a built-in analog modem. The network of analog modems is connected to the public switched telephone network at each precinct using a standard telephone jack. The AV-OS and AV-TSX modems dial a bank of 48 analog modems in the Division of Elections director's office in Juneau, Alaska. The modems establish a communications channel between the voting machine (AV-OS or AV-TSX) and the GEMS server in Juneau. The GEMS software incorporates a communications security feature called secure socket layer (SSL) which encrypts the data transmitted over the modem channel. The Division of Elections operates the communications channels with this feature enabled reducing the likelihood of an eavesdropping attack. At no time is the internet used for communication of or transmission of results.

Appendix J – AccuVote Communications System Description and Appendix K – AccuVote Network Topology provide a system description of the AccuVote communications system. The network schematic provides an overview of the connectivity between each region and the GEMS server in Juneau.

The State of Alaska requires paper ballot as the ballot of record (AS15.15.030 and AS15.15.032). The implementation of this paper ballot in Alaska relies primarily on optically scanned ballot cards which are filled out by each voter. This system has an inherent redundancy which allows a hand count in the case of a total system failure. Although the likelihood of a total system failure is very low, this redundancy ensures that no election will be conducted in which a voter would be unable to cast a ballot at any precinct.

Premier offers an application - Key Card Tool - which is designed to increase the security of AV-TSX memory cards and access cards. The Key Card Tool application allows the Division of Elections to change the passwords and encryption keys on the central administrator, supervisor, and voter access and memory cards. Current passwords and encryption keys are available in the public domain and cannot be considered secure.

Recommendations:

The SOAESP project team did not identify any vulnerabilities requiring remediation in the implementation of the AccuVote communications system. The implementation in use by the Division of Elections is robust and reasonable. It is important to note that all results provided to the public through the transmission of election results are preliminary and must be considered unofficial.

2008 Election Cycle

We recommend implementing the Premier Key Card Tool application to improve the security of the memory cards used in the AV-TSX machines.

We recommend using a GEMS server system that implements the Air Gap Management model (See Appendix M – AccuVote Functional Test Guidelines).

We recommend dedication of a single purpose AV-OS machine for programming AV-OS memory cards in the director's office.

Post Election

Empirical failure data provided by the Division of Elections point to shipping damage as a cause of some hardware failures in the AV-OS machines. It is recommended that improved shipping containers be used to reduce machine stress during transportation. We recommend using secure transport cases, similar to Pelican™ Products 1600 series cases, for transporting AV-OS machines. These cases add a layer of protection against tampering as well as guarding against weather and rough handling. Cases should be locked or sealed. See Appendix I – AccuVote OS Shipping Container Example.

Part 3 Confidence in Outcomes

Section 3.1 – Functional, Logic and Accuracy Testing

Description:

Evaluate processes and procedures the Division of Elections uses for functionality testing and logic and accuracy testing of systems and memory cards.

Summary of Analysis:

The AccuVote election system operated by the Division of Elections requires two different types of testing prior to each election to ensure reliable, error free operation. Functional testing refers to a suite of tests which validate the functional operation of each voting optical scan and touch screen voting machine. Functional testing is required to ensure that the machine will operate as designed on election day. The purpose of functional testing is to identify component failures or issues prior to deployment of the machine for use. Logic and accuracy testing refers to a suite of tests used to validate the error-free operation of the voting machines. The purpose of logic and accuracy testing is to ensure that the ballot programming is accurate and that voter intent is accurately represented in the resulting vote tallies. .

Appendix M is a set of functional test guidelines for the AccuVote system components. The appendix first outlines the functional tests currently implemented by the Division of Elections for each component. A set of recommendations to enhance the functional test suite is then presented. Although the Division of Elections currently performs a subset of the recommended tests it was found that improvements could be made in the test procedures by adding a number of additional tests and by improving the documentation of the test results.

Appendix N is a set of logic and accuracy testing guidelines for the AccuVote system components. The Division of Elections current AccuVote tests procedure can be made more rigorous by following the procedures provided Premier's *State of California: Use Procedures* document. This document provides a comprehensive list of recommendations for secure, error-free use of the AccuVote system. A subset of these recommendations which are applicable to the Alaska's system is outlined in the appendix.

Recommendations:

2008 Election Cycle:

We recommend that the Division of Elections adopt the increased scope of the recommended logic and accuracy test guidelines provided in Appendices M and N. Use of the enhanced procedures decreases the likelihood of an election day failure and reduces the probability of equipment logic or accuracy errors.

Post Election:

We recommend that testing technicians document procedures for revised functional test, logic and accuracy procedures.

We recommend that the guidelines presented in Appendices M and N be used to develop a long-term test documentation system whereby the results of each election cycle's functional, logic and accuracy test results are measured, validated and stored for later access and review.

Section 3.2 – Methods to Improve Voter Confidence

Description:

Identify methods that the Division of Elections can use to improve voter confidence.

Summary of analysis:

Other researchers determined that numerous factors influence public confidence in elections (Celeste, Thornburgh, Lin 2006, Weiser and Goldman 2007). Election administration processes and procedures can directly influence many of these[9] factors.

- Voters' personal experiences at polling places. Research shows that a voter's personal experience is closely related to the level of poll worker training. According to a Pew Trust report (Pew Center on the States 2007), poll worker confidence translates to voter confidence.
- Confidence in election equipment. Closely related to personal experience is voter confidence in election equipment. Most of the concern about election security involves touch screen systems including the AV-TSX machines used in Alaska. In Alaska, each precinct must have a mechanism in place for voters as mandated by the federal Help America Vote Act (HAVA). The AV-TSX touch screen voting systems meet the HAVA requirements. Each of these systems provides a mechanism that allows a voter to verify their individual vote. Additionally votes are recorded on a paper reel inside the touch screen unit that is later verified during a precinct level validation. This paper reel is considered the official paper ballot record. In Alaska, less than 1% of votes are cast on AV-TSX machines. In 2006, five communities used AV-TSX machines for all or most of their votes because these communities would otherwise require a hand-count of paper ballots. However, in most communities very few, if any votes are cast on AV-TSX systems. In Alaska's 2006 general election, in 224 precincts no one used the AV-TSX machines. In 112 precincts, fewer than five voters used the machines.
- Transparency. Alaska has an open process in which observers are encouraged to participate in and observe the entire voting and auditing process. Election procedures are uniform across the state and are written into state statute.
- Availability and frequency of recounts. Alaska has had many close races and frequent recounts. In Alaska, a vote margin less than or equal to 0.5% fewer than 20 votes triggers a recount. Otherwise a candidate or group of ten or more voters may request a recount. The candidate or proposition with the most votes in a

[9] Factors that are beyond the direct influence of election administration procedures are: faith in specific public officials, trust in democratic process, lack of public controversy around election administration, broad acceptance of election systems by social elites, substance and tone of election and political rhetoric, voter technological literacy and knowledge, and election outcome

recount is declared the winner. Since Alaska started using AV-OS machines in 1998, there has never been a case when the recount results changed the election outcome.

- Management of elections by non-partisan elections officials. With the exception of the director of the Division of Elections, Alaska's election officials are employees hired through the state employment process. Most have been working on elections for a long time. We found that several people had tenures of almost 20 years. Regional directors report that many poll workers have long tenures as well.
- Post election audits. The purpose of post-election audits is to give the public confidence that the election machinery is counting votes correctly. The Division of Elections conducts a post election audit, with bi-partisan participation and observers present.
- Paper ballot as the official ballot. According to Alaska state statute, the paper ballot is the official ballot (AS15.15.30 and AS15.15.32). Alaska is one of 35 states that require some form of paper back up. Of the 29 states, 13 use the paper ballots to audit results from electronic tallies (Pew Center for the States 2008, VerifiedVoting.org 2008).

Recommendations:

2008 Election Cycle:

Poll workers need to ensure that if one person uses an AV-TSX machine, at least five voters use it. At least 5 voters need to AV-TSX to protect voter confidentiality. Use the Division of Elections website to encourage members of the public and people concerned about the election system to become observers, encourage people to become poll workers and to make results of this evaluation accessible to the public.

Post Election:

We recommend that the Division of Elections expand its efforts to recruit poll workers and election observers, use the Division’s website and media to inform the public about Alaska’s election system, consider working with high schools to develop a module for teaching about Alaska’s election system and recruiting high-school students to work as poll workers.

Section 3.3 – Metrics and Continuous Improvement

Description:

Establish metrics that the Division of Elections can use as part of a procedure to demonstrate continuous improvement effort regarding of election security and predictability of results over time.

Summary of Analysis:

Sustaining Division of Elections confidence is more likely if a Continuous Process Improvement (CPI) program is instituted. CPI is a structured approach to analyze and identify process improvement opportunities and institute improvements on a continual basis. In the case of the of the voting process, there will always be a need to have, in place, a systematic approach for keeping all levels of the organization involved in changes. The objective would be to keep the staff, equipment, software, procedures and training up to date. An important aspect of CPI is the requirement for criteria to be identified and measured. Measurement becomes the source of metrics on which improvement is based. Throughout the voting cycle, there are opportunities for procedures to collect metrics that, in turn, can be pursued for improvement.

CPI is commonly referenced throughout management and public administration literature and is considered an effective approach for keeping up-to-date and improvements a normal part of the organizational culture. CPI was developed first by Dr. W. Edwards Deming and initial referred to as the "Shewhart cycles". Continuous improvement is accomplished as an iterative cycle that repeats the following steps: Define – Measure – Analyze – Improve – Control. CPI was first applied to quality control in the manufacturing process. The approach is now adapted by many organizations (private and public) for the purpose of involving all organizational levels in improving the quality of services and keeping technologies current (Kelly, 2003; Xenakis and Macintosh, 2006).

An example of a possible criterion for consideration is: "Percent of pre-election testing errors". This is measurable and can be evaluated using a root-cause methodology and subsequent measures indicate improvements. Specific criteria are established as part of the improvement process and reflect the goals of Division of Elections.

The four election regions are not identical and there will always be differences regarding staff experience and voting challenges. There is a need to adopt a methodology within Division of Elections that allows for all of the staff to help in planning and in facilitating improvements in all aspects of the voting process. These include updates in software, equipment, training and related materials. Regional offices need to be involved both because of their contribution to the understanding of unique challenges in the various area of the state and the advantage of having the improvements integrated between regions. All regions improve because of their collective efforts.

Recommendations:

This is to be a change in managerial procedures intended to involve managers at all levels of Division of Elections and will take time to initiate and implement.

2008 Election Cycle:

Very little can be accomplished between now and the end of this election cycle however preliminary objectives, metrics can be explored. Consider conducting an audit during the election to evaluate if these preliminary criteria are the right metrics and use this to collect some baseline data.

Post Election:

Instituting a CPI program should be considered starting in 2009 beginning with overall training of the topics and process of CPI. Next is setting specific improvement goals and measurable criteria. Measurement of results is critical because this becomes the basis for measuring improvements.

We recommend that the regional directors play a role in CPI both because they are close to the unique challenges within the regions and also this involvement facilitates integrating and standardizing the improvements between the regions.

Section 3.4 - Public Input and Commentary

Description:

Provide a weekly review of emails from the public on security issues and summarize and publish general responses to them on the Division of Elections website.

Summary of Analysis:

From September 2007 through end April 2008, six emails were received from members of the public. The suggestions in the emails included:

- Use punch cards that could be fed into an optical scanning system for tallying.
- Hand-count all ballots in the next election.
- Use two-part ballot that would provide a receipt showing the votes cast.
- Eliminate touch screen systems.
- Provide a tear tab with a serial number. Voter could later visit a website to verify correct vote recording using serial number.
- Post results through a website as votes are tallied.
- Set optical scanner to read fainter marks to ensure all legitimate votes can be counted.

Only systems that have been certified by the Election Assistance Commission (EAC) Voting Systems Standards can be used in federal elections. These specifications include detailed requirements pertaining to functional capabilities, hardware standards, software standards, telecommunication standards, security standards, quality assurance standards and system configuration management. Each system certified by the VSS must pass a set of tests performed by an Independent Test Authority (ITA) that has also been certified by the EAC. These standards also include detailed information about ballots and accessibility for voters covered by the American with Disabilities Act (ADA) and HAVA. Currently, by law, systems used in Alaska must conform to the VSS 2002 standard. As new capabilities are developed by election equipment vendors, this equipment must be certified to this minimum standard as well as any then current standard required by law.

At this time, there are no punch card systems that are certified to the VSS standard. Random hand-counts and requests for hand counts for close elections help ensure vote counting accuracy. Election results have never changed as a result of random hand-counts and mandatory or requested recounts.

To protect voter privacy, receipts are not issued. The internet is not considered a secure mechanism for transmitting voting results. At this time, memory cards containing the votes cast on each machine are manually inserted into centralized vote tabulation machines. Real-time information about vote tallies is not provided to ensure that no election results are posted prior to the conclusion of the election. For more detailed

information on the reliability and accuracy of the optical scanning system please see Appendix L – AccuVote Reliability Assessment.

The suggestion to implement a system of tear tabs with serial numbers refers to using cryptographic methods to verify votes. The voter receives an encrypted copy of their voted ballot with a randomized serial number. Voters can use the serial numbers to get internet access to a decrypted version of their voted ballot (Robinson 2004, 2004b). Implementing this process would involve a different system than what is in place. It is one of several innovations worth considering in the event of an overhaul.

2008 Election Cycle:

Continue to monitor feedback through Division of Elections website and respond to frequently asked questions.

Post Election:

Continue to monitor feedback through Division of Elections website. Incorporate suggestions into continuous improvement process (CIP).

Section 3.5 – Absentee Ballot Process

Description:

Provide a description of the absentee ballot process.

Summary Analysis:

Absentee voting is a major component of the election process because, in the last election, 19% of voters voted by absentee. There are two broad categories of absentee voting. The first category includes absentee by mail, fax and special advanced requests. The second category is called "in-person absentee" It includes special needs voting, early voting and absentee in person voting.

In all cases, the process starts with the Division of Elections' request for ballots to be printed. Absentee ballots are produced as part of the same purchase order to the printer order for precinct voting ballots. It is placed 48 days before the election. The ballots are numbered in sequence with numbers of ballots printed from estimates based on previous elections. State of Alaska statute requires that all absentee ballots be reviewed, opened and counted by the 15th day after the election. Absentee ballots are not part of the post-election audit process.

Absentee voting information is detailed on the State of Alaska, Division of Elections web site and procedures for the various categories are outlines in: Absentee Voting Station Official Procedures (Rev. 5/2006) and Absentee Voting Official's Handbook (Rev. 4/25/06). Regarding both categories of absentee voting, the Division of Elections has carefully delineated the open period for the respective absentee voting as well as the process and procedures for voting absentee. We identified one issue unique to absentee voting that requires special attention: *time exposure*. The ballots are in distribution, storage and most importantly, in use, over many more days than the ballots and machines used specifically at a polling place on election day.

Appendix Q - Summary of Absentee Voting delineates types of absentee voting and respective pre- and post-election dates of the process.

Recommendations:

2008 Election Cycle:

All of the security issues with regard to memory cards, upgrades and ballots used at polling places for election day also apply to absentee voting. Ballots stored for use in absentee voting need to have tight security to avoid loss, damage or tampering along with procedures and staff training emphasizing the risks of unauthorized access. Procedures for "end-of-day" documentation, distribution, ballot storage and shipping, and final

delivery of ballots and reports to Division of Election in Juneau need special attention to assure adequate control and accountability (see Appendix H – Security Training).

Post Election:

The voting equipment used in support of the absentee voting processes should be identified in general usage/maintenance records should the need arise to assess unusual usage, security concerns and/or maintenance patterns.

Section 3.6 – Random Sampling Methodologies

Description:

Research other random sampling methodologies that might provide additional confidence in election results. These recommendations would be proposed for further consideration and evaluation.

Summary of analysis:

Random sampling methodologies refer to sample size and how ballots are chosen for hand counts in Alaska's post election audit.

The main purpose of the post election audit is to increase public confidence in election results. Audits do this by verifying that the machine counts were correct and confirming that a manual recount would not change the outcome. Audits also detect tampering with the system, detect large scale systemic errors, deter fraud, and provide feedback to allow jurisdictions to improve voting technology and election administration (Norden 2007). The random sample should be large enough to be able to detect discrepancies but small enough to be efficient so that hand counts don't take a long time. Alaska is one of only 12 states with an election audit (Norden 2007) program. Many states are currently evaluating and pilot testing audit procedures and sampling methods. But to date, there is little agreement about which is the best audit procedure (Norden 2007).

One of the benefits of a uniform statewide system in Alaska is that observers only need to go to one place to see the audit. Alaska's random selection process is transparent. Bi-partisan review board members select the random sample by drawing precinct numbers from strips of paper in a box. Precincts are eligible for selection if they include at least 5% of the voters in that House district. In Alaska, a bi-partisan review board hand counts ballots from one precinct in each house district. If the results of the hand count differ from the results from electronic counts by more than 1%, all ballots in that House district must be hand counted. To date, there has never been a case where counts differed by more than 1% in any precinct.

Recommendations:

2008 Election Cycle:

No changes this year.

Post Election:

Wait to consider changes until audit evaluations in other states are finished. Any changes to the procedure would require legislative approval since the audit procedure is written into Alaska state statutes.

Conclusions

The following table summarizes our main recommendations, some of which the Division of Elections could put into effect before the August primary and the November general election, and some of which it can't.

Recommendations for Improving Alaska's Election Security

Change By 2008 Election	Why?	Change After Election	Why?
✓ *Verify the accuracy of voting technology before and after the election, by comparing code in voting machines with correct, registered code* ✓ *Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines* ✓ *Change passwords on all voting technology throughout the system* ✓ *Use tamper-evident seals on shipping cases and envelopes* ✓ *Add election-security material to poll workers' training manual* ✓ *Increase vigilance about security procedures in absentee polling locations* ✓ *Purchase state-owned voting machines for use in North Slope Borough, rather than borrowing borough-owned machines*	This series of changes in technology and election procedures will make the existing technology more secure; improve security procedures among election officials and poll workers; and help increase Alaskans' confidence in the integrity of state elections. These measures can all be taken in the short-term, before the August primary and the November 2008 election.	✓ *Upgrade voting machines and other technology to new, improved platform* ✓ *Establish long-term security goals and a method for measuring progress* ✓ *Improve testing processes to insure all voting technology is functioning properly and recording votes accurately* ✓ *Develop and implement a standard plan for tracking and changing passwords* ✓ *Improve system for tracking the number and location of voting machines, through bar-codes or other inventory-control measures* ✓ *Strengthen storage facilities for voting machines and other system components with dead-bolt locks, alarms, ceiling grids, self-locking doors, and other features to prevent forced entry* ✓ *Buy more-secure shipping containers for optical-scanners* ✓ *Recruit and train more poll workers* ✓ *Consider partnerships with other institutions to do ongoing evaluation and implementation of changes in election-security technology*	Installing the new platform is the single-most important change the state can make, because it will reduce or eliminate risks of vote-tampering identified in the current system. But the platform must first be certified to the Election Assistance Commission's 2002 Voting System Standards, and after that will require an estimated 1,000 man-hours to install on election equipment statewide. Even if it were certified soon, it is not practical now to install the upgrade before the 2008 elections, given the time, expenses, and logistics involved. The other post-election recommendations are either longer-term enhancements of measures recommended for 2008, or additional security measures that there isn't time enough to implement before the 2008 elections.

- Upgrade to the new, more secure platform after the election. We can't over-emphasize the importance of this upgrade. Alaska, California, Florida, and other states use the same or similar voting technology. Election-security studies in several states found that the existing technology was potentially vulnerable to vote-tampering in a number of ways. The new platform, Premier Election Systems Assure 1.2, which the manufacturer developed in response to those studies, is still being tested to insure that it meets standards set by the federal Election Assistance Commission. We had hoped the system could be installed on Alaska's voting equipment by the 2008 election, but we now believe that's not feasible. Alaska is now in the run-up to the August primary and the November election. The Division of Elections is programming its equipment for those elections and doing other work that has to meet specific pre-election deadlines. Also, because the state shares voting equipment with local governments, the upgrade will have to be coordinated with them as well. To add it is a huge, expensive job requiring complicated logistics at this point is not feasible. But we recommend that it be done as soon as possible after the election.
- Establish security goals and a method for regularly measuring progress toward those goals. The Division of Elections is well aware of security issues, and has taken a number of steps to improve security. But it currently has no long-range security goals, nor a plan for measuring progress. We believe it's very important for the division to develop such goals and systematically meet them.
- Consider forming a partnership with some other organization that could continuously monitor and evaluate any new election-security vulnerabilities and ways to improve security. This would allow the Division of Elections to quickly make any necessary changes or improvements, before problems developed. Some states are already doing this. The Division of Elections itself does not have adequate staff to do such monitoring.
- Install new software that allows election officials to create a more-secure password authentication system for touch-screen machines. Election officials are in fact already installing this new software, as they do programming for the upcoming election. This new software, called Key Card Tool, allows them for the first time to create their own authentication password and encryption keys for the state's 439 touch-screen machines. This is a substantial improvement in security. Previously, the default password and keys were in the public domain. They were programmed into all the touch-screen machines and couldn't be changed. Now, the password and keys can be changed regularly, and over time election regions could have their own individual passwords and keys.
- Verify the accuracy of voting technology. Before and after the November election, election officials should test all voting machines by comparing code in the machines with correct, registered code. In the longer-term, the state should develop standard testing processes to insure all voting technology is functioning properly and recording votes accurately.

- Change system passwords. Before the election, the state should change all passwords currently used in election-system technology. After the election, the state should develop a plan for routinely tracking and changing passwords.
- Use tamper-evident seals on envelopes and shipping containers. This precaution can be taken before the upcoming election. Critics argue that attackers could in fact open such seals without leaving any evidence of tampering. But we believe that especially in Alaska—where ballots and equipment can travel long distances under difficult conditions—tamper-evident seals do help improve security.
- Recruit more poll workers and improve their election-security training. Before the election, the Division of Elections should add a section on election-security to the existing training manual, which doesn't currently discuss security. In the longer term, the state needs to recruit more poll workers—which in itself would help improve security in polling places—and to provide better training (possibly online) in election-security procedures.
- Improve the way voting machines are transported, tracked, and stored. Most of these recommended improvements can't be made until after the November election. They include buying better shipping containers for optical-scan machines, which have to be shipped to many small communities from larger regional centers before and elections and returned afterward. The state also needs a better system for tracking the number and location of voting machines, through bar-codes or other methods of inventory-control. Also, the physical security of machines in storage needs improvement. The state should consider reinforced doors, dead-bolt locks, ceiling grids, alarms, and other measures as appropriate.

We have made a number of recommendations for improving the security of Alaska's election system, but we want to keep those recommendations in context: Alaska's election system is in good shape. Other states are now adopting measures we've had in place for years. Personnel of the Division of Elections understand the system and have a good idea of what kinds of measures could help make it more secure.

But there's always room for improvement. Aside from the specific recommendations we've listed, Alaska needs to build a foundation for the future—to make sure Alaska's election system stays among the best in the country. The current election technology is aging, and the state will face new choices when it has to upgrade that technology. It needs to start systematically assessing its future needs and new technologies now.

Proposed Statement of Work for Phase 3: Implementation

1. Investigate Institutional Partnership
2. Develop revised functional, logic and accuracy testing procedures
3. Continue to monitor poll-worker training and auditing programs going on in other states (grant-based work being done) including on-line training capabilities.
4. Develop Assure 1.2 upgrade procedure.
5. Perform Assure 1.2 cost benefit analysis for implementation methodology
6. Design process to audit use of and results from implemented recommendations.
7. Develop procedures for recommended technical enhancements (e.g. hash code)

References

Alvarez, R. Michael & Hall, Thad E. (2005, June). *Public attitudes about election governance*. University of Utah, Center for Public Policy and Administration and Caltech/MIT Voting and Technology Project.

Alvarez, R. Michael. (2005, October 5). *Precinct voting denial of service*. Paper prepared for NIST (National Institute of Standards and Technology) Threats to Voting Systems workshop. Caltech-MIT Voting Technology Project.

Bishop, Matthew. (2007). California red team review of Diebold voting system. *State of California Top-to-Bottom Review.*

Calandrino, Joseph A., Feldman, Ariel J., Halderman, J. Alex, Wagner, David, Yu, Harlan, Zeller, William P. (2007, July 20). *Source code review of the Diebold voting system.*

California Secretary of State. (2007, October 17). *Withdrawal of approval and conditional reapproval of Diebold Election Systems, Inc. GEMS 1.18.24/AccuVote-TXS/AccuVote-OS DRE and optical scan voting system.*

California Secretary of State. (2007, October 25). *Post-election manual tally requirements.*

Celeste, Richard, Thornburgh, Dick, & Lin, Herbert (Eds.). (2006). *Asking the right questions about electronic voting.* Washington, DC: National Academies Press.

Diebold Election Systems. (2007, August 22). *Report of Diebold Election Systems, Inc. (DESI) to California Secretary of State Red Team report issued on the GEMS 1.18.24/AccuVote-TSX/AccuVote-OS/DRE & optical scan voting system.*

Diebold Election Systems. (2004). *GEMS 1.18 product overview guide* (Revision 2.0).

Diebold Election Systems. (2005). *AccuVote-TSX ballot station 4.6 user's guide* (Revision 2.0).

Diebold Election Systems. (2005). *AccVote-OS Precinct Count 1.96 user's guide* (Revision 4.0).

Diebold Election Systems. (2005). *GEMS 1.18 user's guide* (Revision 12.0).

Diebold Election Systems. (2006). *Verifying EPROM program file versions for the AccuVote-OS product* (Revision 2.0).

Diebold Election Systems. (2007, January 11). *Client security policy* (Revision 6.0).

Diebold Election Systems. (2007). *Key card tool 4.6 user's guide* (Revision 4.0).

Diebold Election Systems. (n.d.). *Response and solutions to system review recommendations.*

Diebold Election Systems. (n.d.). *Verifying GEMS hash key quick reference guide.*

Gardner, R., Yasinec, A., Bishop, M., Kohno, T., Hartley, Z., Kerski, J., et al. (2007). *Software review and security analysis of the Diebold voting machine software.* Florida State University, Security and Assurance in Information Technology Laboratory.

Johnston, Roger G. (2006, Nov-Dec). Tamper-indicating seals. *American Scientist, 1*. p 515-523.

Kiayias, Aggelos, Michel, Laurent, Rusell, Alexander, Shashidhar, Narasimha, See, Andrew, Shvartsman, Alexander, et al. (2007, December). *Tampering with special purpose trusted computing devices: A case study in optical scan e-voting*. Paper presented at the 23rd Annual Computer Security Applications Conference, Miami Beach, Florida.

Kuo, C., Romanosky, S., & Cranor, L. (2006). Human selection of mnemonic phrase-based passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)* (pp. 78-78). Pittsburgh, PA: ACM Press.

Norden, Lawrence D., & Lazarus, Eric. (2007). *The machinery of democracy: Protecting elections in an electronic world*. Chicago: Academy Chicago Publishers.

Pew Center on the States. (2007, September). *Helping Americans vote: Poll workers*.

Pew Center on the States. (2007). *The Help America Vote Act at 5*.

Premier Election Solutions. (n.d.). *Premier master equip acceptance test procedures 012008.xls*.

Premier Election Solutions. (2007). *Plan on formatting and clearing program storage on Voting System* (Revision 1.0).

Premier Election Solutions. (2007). *Premier's Windows configuration guide* (Revision 3.0).

Premier Election Solutions. (2007). *State of California use procedures*.

Premier Election Solutions. (2008). *AccuVote-OS hardware guide* (Revision 13.0).

Premier Election Solutions. (2008). *AccuVote-TSX hardware guide* (Revision 13.0).

Premier Election Solutions. (2008, January 17). *California tamper evident security seal document* (Version 2).

RABA Technologies LLC. (2004, January 20). *Trusted agent report, Diebold AccuVote-TS voting system*. Retrieved March 21, 2008 from http://www.raba.com/press/TA_Report_AccuVote.pdf.

Rausand, R., & Hyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Robinson, Sarah. (2004, March). What's so special about voting? *SIAM (Society for Industrial and Applied Mathematics) News, 37* (2).

Robinson, Sarah. (2004, April). Works in progress: trustworthy cryptographic voting systems. *SIAM (Society for Industrial and Applied Mathematics) News, 37* (4).

Shamos, Michael Ian. (1993). *CFP'93 Electronic voting--evaluating the threat*. Retrieved October 15, 2007 from http://euro.ecom.cmu.edu/people/faculty/mshamos/CFP93.htm

Shamos, Michael Ian. (2004). *Paper v. electronic voting records—an assessment*. Retrieved October 15, 2007 from *http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm*

Spafford, E. (2006, April 19). *Security myths and passwords*. CERIAS (The Center for Education and Research in Information Assurance and Security). Retrieved March 21, 2008 from http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/

State of Alaska, Division of Elections. (2007). *Accu-Vote security enhancements and features.*

State of Alaska. (2006). *Alaska Statutes. Title 15: Elections*. Charlottesville, VA: Matthew Benders & Company, Inc.

State of Alaska. (2006). *Polling place election procedures. Hand count and* touch screen precincts.

State of Alaska. (2006). *Polling place election procedures. Optical scan and touch screen precincts.*

State of Alaska, Division of Elections. (n.d.). *Closing the polls, Accu-Vote optical scan unit transmitting results.*

State of Alaska, Division of Elections. (n.d.). *LAT testing and memory card preparation instructions.*

State of Alaska, Division of Elections. (n.d.). *Pre-Election cycle optical scan functionality testing.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board LAT report log.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test early voting memory card – general election.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test early voting memory card – primary election.*

State of Alaska, Division of Elections. (n.d.). *Regional AccuVote board touch screen logic and accuracy test precinct memory card – primary election.*

State of Alaska, Division of Elections. (2006). *Specifications for Division of Elections ballot transportation and security for the 2006 general elections.*

State of Missouri, (2007). *It's your turn: be a poll worker – 2007 survey results*.

Technical Guidelines Development Committee. (2007). *Voluntary Voting System guidelines recommendations to the Election Assistance Commission.* Technical Guidelines Development Committee.

Thompson, Clive. (2008, January 6). Can you count on voting machines? *The New York Times.*

U.S. Election Assistance Commission (EAC). 2006. *Election crimes: An initial review and recommendations for future study*. Washington D. C.

U.S. Federal Election Commission. (2002). *Voting system standards, Volume I: performance standards.* Washington, DC:

Weiser, Wendy R., & Goldman, Johan. (2007). *An agenda for election reform*. New York University School of Law, Brennan Center for Justice.

UNIVERSITY of ALASKA ANCHORAGE

State of Alaska Election Security Project

Phase 2 Report Appendices

Prepared for Lieutenant Governor Sean Parnell
and the State of Alaska Division of Elections

May 16, 2008
Final Report

This page left intentionally blank

Appendix A - Assure 1.2 Upgrade Labor Estimate					
Item Number	*Assure 1.2 Software or Firmware Component*	*Upgrade Procedure Description*	*Machines Affected*	*Estimated Hours Per Machine*	*Total Hours*
1	AV-OS Firmware Upgrade	Existing 1.96.6 firmware EPROM is physically replaced with 1.96.10 firmware EPROM. New EPROM to contain a serial number on bottom side of chip.	290	0.25	73
2	AV-TSX Bootloader Upgrade	Existing BLR 7.1.2.1 Bootloader software is upgraded to BLR 1.3.9	439	0.25	110
3	AV-TSX Windows CE Upgrade	Existing Windows CE operating system software is upgraded from the current version 4 10.2.1 to version 4 10.3.9	439	0.25	110
4	AV-TSX BallotStation Upgrade	Existing BallotStation software is upgraded from the current version 4.6.4 to version 4.7.2	439	0.25	110
5	AV-TSX AccuView Printer Module Software Upgrade	Existing AccuView printer modules software is upgraded from the current version model 3 rev. 3.03 to model A rev 3.03	439	0.25	110
7	GEMS Election Management Software Upgrade	Existing election management software is upgraded from the current version 1.18.24.0 to version 1.20.2	8	8	64
8	Key Card Tool Software Upgrade	The Key Card Tool software must be upgraded to version 4.7.1	2	8	16
9	Voter Card Encoder Upgrade	The voter card encoders must be upgraded from the existing version 1.3.2 to the Assure 1.2 version 1.3.3	1198	0.25	300
10	VC Programmer Software Upgrade	The VC Programmer software must be upgraded from the existing version 4.6.1 to the Assure 1.2 verion 4.7.1	System-level task	lot	4
11	Assure 1.2 Upgrade AV-OS Procedure Development	Develop and draft a plan and a procedure for upgrade of all AV-OS, AV-TSX and GEMS machines to include acceptance and functional testing following the upgrade procedure implementation.	System-level task	lot	100
				Total Hours	**995**

Appendix B - Assure 1.2 Upgrade Analysis

1. System Overview

The Premier Election Solutions AccuVote system used by the State of Alaska Division of Elections (DoE) is comprised of several different software and hardware components. These software and hardware components interact at different times during an election in order to allow election officials to prepare ballots and races, to allow voters to cast ballots and to allow election officials to tabulate the results of the election.

The State of Alaska DoE utilizes the following Premier system components in its implementation of the AccuVote election system.

1.1 AccuVote Optical Scan Model B (AV-OS)

The AccuVote Optical Scan (AV-OS) hardware is available in two different firmware configurations, precinct count and central count. The State of Alaska DoE does not use the Premier Election Solutions central count firmware.

The precinct count firmware version of the AV-OS is used by individual precincts to conduct elections and tally votes. The firmware in each AV-OS machine is stored on an Electrically Programmable Read Only Memory (EPROM) device which is accessed by the AV-OS hardware. The system utilizes a re-writable 40-pin Epson memory card to program individual elections. Tallied votes and ballot definition files are stored on the memory card. A precinct AV-OS machine reads the election mode from the memory card and adopts that functional mode for operation.

The firmware revision currently present on the AV-OS platform operated by the State of Alaska DoE is precinct count 1.96.6.

1.2 AccuVote Touchscreen Model D (AV-TSX)

The AccuVote Touchscreen (AV-TSX) hardware used by the State of Alaska DoE is a Direct Recording Electronic (DRE) machine with an additional module which produces a Voter Verifiable Paper Audit Trail (VVPAT). The AV-TSX machine allows voters to cast their votes from an electronic touchscreen interface. Once the ballot is cast the touchscreen device sends the ballot to a VVPAT printer where the voter validates the results. Once the voter accepts the printed ballot the vote is considered cast and the tallies are updated on the electronic memory card.

The AV-TSX machine requires two different applications to run. The bootloader application is used to load the Windows CE operating system image from the system flash memory. The State of Alaska DoE currently uses Bootloader v.BLR 7.1.2.1. The system also requires the BallotStation application which runs under the Windows CE operating system. This application implements the voter interface and administrative functionality within the AV-TSX machine. The State of Alaska DoE currently uses BallotStation v.4.6.4.

An additional security enhancement is available from Premier Election Solutions for use with the AV-TSX machines. The security enhancement is called Key Card Tool. Key Card Tool is

a software application which allows election officials to change encryption keys and access passwords within the AV-TSX system. The State of Alaska DoE is in the process of implementing the Key Card Tool application for the 2008 election cycle.

1.3 GEMS (Global Election Management System)

The Division of Elections utilizes a total of eight (8) GEMS servers distributed across the State of Alaska. The GEMS servers implement the ballot definition, vote tabulation and system reporting functions for the Premier Election Solutions AccuVote system.

Currently, the Division of Elections is operating identically configured Dell PowerEdge Servers which run the Premier Election Solutions GEMS applications.

The GEMS systems are running Election Management System v.1.18.24.0

In addition to running the Election Management System software, the system is operating with Dell BIOS A09.

The Division of Elections does not currently calculate hash codes of the certified software running on the GEMS servers.

1.4 Assure 1.2 Components

The Assure 1.2 software / firmware upgrade is a complete system revision. This system revision is comprised of several different software and firmware components which must be loaded on to each hardware platform in order to obtain a complete system upgrade.

1.4.1 AV-OS Components

The AV-OS model B machines must be upgraded from the existing 1.96.6 EPROM firmware revision to the AV-OS Precinct Count Firmware version 1.96.10 (build date 10-01-2007).

1.4.2 AV-TSX Components

The AV-TSX model D machines must be upgraded from the existing Bootloader v.BLR 7.1.2.1 to the Assure 1.2 Bootloader v1.3.9 (build date 11-19-2007).

The AV-TSX model D machines must be upgraded from the existing Windows CE version v.4 10.2.1 to the Assure 1.2 v.4 10.3.9 (build date 1-19-2007),

The AV-TSX model D machines must be upgraded from the existing BallotStation v.4.6.4 to the Assure 1.2 BallotStation v.4.7.2 (build date 01-07-08).

The AV-TSX model D machines must have the AccuView Printer Module software updated from AVPM model 3 Rev 3.03 o the Assure 1.2 AVPM model A v.3.03 (build date 11-01-07).

1.4.3 GEMS Components

The GEMS Servers must be updated from the existing Election Management Software v.1.18.24.0 to the Assure 1.2 v.1.20.2 (build date 11-19-2007).

The GEMS Servers must be updated to the Assure 1.2 Security Manager v.1.0.5 (build date 01-15-2008).

1.4.4 System-wide Components

The AV-OS model B machines and the AV-TSX model D machines must have the AccuBasic Report Files version updated to v.2.2.3 (build date 11-19-2007).

The Keycard Tool software must be updated to Assure 1.2 Keycard Tool v.4.7.1 (build date 11-01-2007).

The Voter Card Encoder must have the existing software v.1.3.2 updated to the Assure 1.2 Voter Card Encoder v.1.3.3 (build date 11-01-2007)

The VC Programmer must have the existing software v.4.6.1 updated to the Assure 1.2 VC Programmer v.4.7.1 (build date 11-01-2007).

1.4.5 Assure 1.2 Release Notes

At the time that this document was drafted the Premier Elections Solutions software had not yet been certified to the VSS 2002 standard. As such the Assure 1.2 release notes are not yet available for review.

2. Assure 1.2 Upgrade Cost Estimate

2.1 Assure 1.2 Software Cost Estimate

The State of Alaska Division of Elections has a current maintenance agreement with Premier Election Solutions, Inc. Software upgrades are provided to the Division of Elections at no additional cost while the maintenance agreement is in effect.

2.2 Installation and Validation Cost Estimate

The installation and acceptance testing of the Assure 1.2 upgrade represents a significant dedication of time by the Division of Elections. Upgrade from the existing AccuVote system revision to the Assure 1.2 revision requires the execution of ten individual tasks. A rough estimate of the labor hours associated with the implementation of each Assure 1.2 component is provided in “Appendix A – Assure 1.2 Upgrade Labor Estimate”.

3 Assure 1.2 Software Evaluation

Phase 1 of the SOAESP identified a number of different system issues presented by the California Source Code Review of the Diebold Voting System (Calandrino, et al. 2007), the California Red Team Review (Bishop, 2007), the Florida Software Review and Security Analysis of the Diebold Voting Machine Software (Gardner, et al., 2007) and others. As a result of this analysis, the State of Alaska is interested in evaluating Premier Election System's Assure 1.2 software release. This new release of software is applicable to the State of Alaska's AccuVote system.

The purpose of this section is to evaluate the Assure 1.2 software platform against the list of issues, vulnerabilities and problems identified in Phase 1. Recommendations are made regarding the installation of the Assure 1.2 on Alaska's AccuVote system.

3.1 VSS 2002 Compliance

The Premier Election Solutions Assure 1.2 is currently undergoing evaluation by the nationally recognized testing laboratory Systest. Premier Election Solutions, Inc. is confident that the Assure 1.2 software release will be compliant with the Voting System Standards 2002 certification requirements. Certification under the VSS 2002 requirements has not yet been received. State of Alaska law requires that the system be certified prior to installation on the production voting system.

3.2 California Red Team Review

The California Red Team Review (Bishop, 2007) identified a number of issues which are addressed by Premier in the Assure 1.2 platform. These issues are outlined below:

3.2.1 Precinct Count AV-OS Ballot Tampering

The California Red Team was able to verify previous results wherein the ballot totals in the AV-OS memory card could be tampered with to affect the outcome of an election.

The Assure 1.2 software release corrects this issue.

3.2.2 AV-TSX Malware

The California Red Team verified previous findings in which a malicious user might overwrite system firmware and / or software. The potential impact of this type of vulnerability was presented in the Red Team Report.

The Assure 1.2 software release corrects the bootloader issue. Premier believes that the format string error issue does not present a real vulnerability.

3.2.3 AV-TSX Escalation of Privileges

The California Red Team identified a vulnerability in which a malicious user might gain access to the system at the supervisor or central administrator level.

The Assure 1.2 software release corrects this issue. The user can still enter the system setup / diagnostics mode when a peripheral device failure occurs. Administrative functions are denied.

3.2.4 AV-TSX Default Static Key

The California Red Team commented in their report on the use of the default static authentication and data keys within the AV-TSX system.

The Premier Election Solutions Keycard Tool application should be used to increase the security surrounding smart card use in the AV-TSX system. Premier Election Solutions believes that Indication of the default key on the AV-TSX interface is a security feature. The Assure 1.2 software release updates the Keycard Tool application to version 4.7.1.

3.2.5 GEMS Databases

The California Red Team identified an issue with database access within the GEMS server where a malicious user could gain access to the GEMS databases and corrupt or manipulate the contents of the database.

The Assure 1.2 software release corrects the direct database direct read / write issue and improves database security.

3.2.6 GEMS Audit Logs

The California Red Team found that the audit logging functionality within the GEMS server was insufficient to identify all malicious user activity.

The Assure 1.2 software protects the election database using password access.

3.3 Florida Software Review

The Florida review team (Gardner, et al., 2007) identified a number of issues with the Premier Election Solutions hardware and software. The text below describes issues which were identified by the Florida team as requiring input and resolution by Premier Election Solutions.

3.3.1 RSA Hardware Signature Flaw

The Florida evaluation team found that the AV-OS and AV-TSX RSA encryption signatures which validate the AccuBasic scripts in the system firmware are implemented in a manner which is susceptible to malicious attack.

The Assure 1.2 software release corrects the hardware signature flaw.

3.3.2 AV-OS Memory Card Integrity Is Not Protected

The Florida evaluation team found that the AV-OS memory card contents are not encrypted or authenticated in any manner. This vulnerability was found to expose the AV-OS platform to attack.

Premier Election Solutions believes that a complete memory card authentication implementation is beyond the capabilities of the AV-OS hardware. Improvements relating to AccuBasic report scripts have been implemented. Physical memory card protection is recommended as a top security priority.

3.3.3 AV-TSX Cryptographic Key Management

Like the California Red Team, the Florida evaluation team found that the AV-TSX was vulnerable to smart card attacks when using the default data and security keys within the AV-TSX system.

The Premier Election Solutions Keycard Tool application should be used to increase the security surrounding smart card use in the AV-TSX system. The Assure 1.2 software release updates the Keycard Tool application to version 4.7.1.

3.3.4 AV-TSX Memory Card Update File is Unprotected

The Florida evaluation team found that the assure.ini file was not sufficiently protected within the AV-TSX system. This lack of protection was found to expose the system to malicious attackers.

The Assure 1.2 software release corrects this issue.

3.3.5 AV-TSX Smart Card Authentication Uses Only a Hard Coded Password

The Florida evaluation team found that even with the use of the Keycard Tool application the AV-TSX system was vulnerable to smart card attacks by skilled attackers.

Not addressed by the Assure 1.2 software release. Premier Election Solutions believes that the vulnerability identified in the Florida analysis can be satisfactorily mitigated by training election workers to identify and act on suspicious activity in the polling place.

3.3.6 AV-TSX Supervisor PIN is Not Cryptographically Protected

The Florida evaluation team found that even with the use of the Keycard Tool application the AV-TSX system was vulnerable to smart card attacks by skilled attackers.

Not addressed by the Assure 1.2 software release. Premier Election Solutions believes that the supervisor PIN is sufficient to protect supervisor access and that procedural checks should be implemented which restrict access to the supervisor cards.

3.3.7 AV-TSX Insecure Storage Mount

The Florida evaluation team found that the storage device within the AV-TSX platform was not implemented in the most secure manner possible. This vulnerability exposes the system to vote tampering attacks by malicious users.

The Assure 1.2 software release corrects this issue.

3.3.8 AV-TSX System Configuration Information is Unprotected

The Florida evaluation team found that a large portion of the system configuration for the AV-TSX platform is stored in the system registry. Alteration was found to be feasible by a malicious user.

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that a security risk is posed by this issue.

3.3.9 AV-TSX Ballot Definition File is Unprotected

The Florida evaluation team found that the ballot definition file uses an encryption method which is not considered to implement the highest level of security.

The Assure 1.2 software release addresses this issue by increasing the security of the ballot definition file protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.10 AV-TSX No Integrity Protection of Stored Electronic Ballots

The Florida evaluation team found that the encryption method used to secure the election database file was not implemented in the most secure manner possible. The Florida team made recommendations to Premier Election Solutions regarding security enhancements.

The Assure 1.2 software release addresses this issue by increasing the security of the stored electronic ballot file protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.11 AV-TSX Ballots are Stored Sequentially

The Florida evaluation team found that the ballots are stored within the AV-TSX system in the order in which they are cast. Users with encryption key access could potentially correlate voters to ballots and undermine the anonymity of the election.

The Assure 1.2 software release does not address this issue. Premier believes that in order to exploit this issue the malicious user would require access to the encryption keys within the AV-TSX system. The encryption keys are not externally accessible by the user and as such Premier believes that this issue does not represent a vulnerability.

3.3.12 AV-TSX Candidate Information is Not Stored in the Results File

The Florida evaluation team found that the candidate information on a ballot is not stored and a malicious user might use this vulnerability to tamper with vote counts.

The Assure 1.2 software release does not address this issue. Premier believes that this is not a security vulnerability.

3.3.13 AV-TSX Audit Logs Are Not Cryptographically Protected

The Florida evaluation team found the AV-TSX audit logs are protected in the same manner as the electronic ballots. Improved encryption methods exist and are outlined by the Florida team.

The Assure 1.2 software release addresses this issue by increasing the security of the AV-TSX audit log protection using HMAC-SHA-1 (Hash Message Authentication Code Secure Hash Algorithm 1).

3.3.14 AV-TSX Data is Neither Authenticated Nor Encrypted Over the Communication Link

The Florida evaluation team found that although SSL an available protocol within the system its use is optional. Further, the Florida team found issues with the Premier Election Solutions implementation of the SSL protocol.

The Assure 1.2 software release corrects this issue. Florida reviewers found that the implementation of the SSL protocol was not initialized with sufficient entropy to ensure secure communications. The Assure 1.2 software increases the entropy of the SSL protocol seed.

3.3.15 AV-TSX Bootloader Automatically Replaces Itself

The Florida evaluation team found that the bootloader process automatically replaced itself if a new copy of the bootloader file was found on the memory card. The Florida team made recommendations to improve the security of the bootloader replacement process.

The Assure 1.2 software release corrects this issue. Updating the bootloader software now requires both operator and bootloader software authentication.

3.3.16 AV-TSX Bootloader Automatically Replaces Operating System

The Florida evaluation team found that the AV-TSX bootloader could cause the operating system to be replaced if certain file types were found on the system memory card.

The Assure 1.2 software release corrects this issue. Updating the operating system now requires both operator and operating system software authentication.

3.3.17 AV-TSX Bootloader Automatically Runs .ins File on the Memory Card

The Florida evaluation team found that the AV-TSX bootloader automatically ran files with an extension of .ins. Although the .ins files on the memory card are signed the Florida team found the signatures to have vulnerabilities within the AV-TSX system.

The Assure 1.2 software release corrects this issue. The software now requires authentication of the user and of the .ins file proper to execution of .ins files.

3.3.18 AV-OS Leaks Memory Card Contents

The Florida evaluation team found that the contents of an AV-OS memory card could be obtained by interfacing a laptop computer to the AV-OS and using built-in Microsoft Operating System tools.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that this vulnerability can be mitigated by the physical security measures of locking the AV-OS onto the ballot box and by locking the Yes / No keys on the AV-OS machine.

3.3.19 AV-OS Supervisor PIN Not Cryptographically Protected

The Florida evaluation team found that the supervisor access PIN was vulnerable to attack by a malicious user if the user was familiar with the method used to secure the supervisor access PIN.

The Assure 1.2 software release does not address this issue. Hardware limitations within the AV-OS platform do not allow for secure supervisor PIN storage. Premier Election Solutions recommends that users implement procedural security mitigations by strictly controlling supervisor card access.

3.3.20 AV-OS No Authentication Between GEMS and the Terminal

The Florida evaluation team found that no authentication exists on the communications channel between the AV-OS and the GEMS server.

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a security vulnerability because the upload of data to the GEMS system is intended for the release of unofficial results only.

3.3.21 AV-OS Attacker Can Hide Pre-loaded Votes

The Florida evaluation team found that multiple different attacks existed in which the ballot count could be compromised. The attacks formulated were based on the previously identified weaknesses in the security key implementation and memory card integrity.

The Assure 1.2 software release corrects this issue. Details about how this issue was corrected were not provided by Premier Election Systems.

3.3.22 AV-OS Vote Counters Are Not Directly Checked for Overflow

The Florida evaluation team found that the vote counters associated with individual candidates were not checked for overflow and were thus subject to potentially insecure conditions. Not specific attacks were presented.

The Assure 1.2 software release corrects this issue. Details about how this issue was corrected were not provided by Premier Election Systems.

3.3.23 AccuBasic Interpreter Faults

The Florida evaluation team identified a number of different AccuBasic issues in their reports which either compromise or reduce system security. These issues are:

3.3.23.1 Error Checking is Inadequate

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a vulnerability.

3.3.23.2 Error Codes Returned by the AV-OS System are Ignored

The Assure 1.2 software release does not address this issue. Premier Election Solutions does not believe that this is a vulnerability.

3.3.23.3 Unchecked String Operation: Allows Overwrite of Stack Memory

The Assure 1.2 software release corrects this issue. Premier Election Solutions did not provide details about how this vulnerability was addressed.

3.3.24 GEMS AccuBasic Scripts are Not Authenticated on the GEMS Server

The Florida evaluation team found that the GEMS server does no checks on the AccuBasic bytecode. All bytecode validation is performed from within the AV-OS and AV-TSX platforms using the encryption signatures. The Florida team previously found the signatures used to have vulnerabilities.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that the authentication of the AccuBasic scripts on the AV-OS and AV-TSX platforms is sufficient to ensure security.

3.3.25 GEMS Password Does Not Protect Access to GEMS or Audit Logs

The Florida evaluation team found that using a simple, publicly known attack, access to the GEMS database and audit logs could be obtained from within the Windows Operating System.

The Assure 1.2 software release corrects this issue. Database access within the Assure 1.2 software release is password protected.

3.3.26 GEMS Incomplete Implementation of the SSL Protocol

The Florida evaluation team found that the use of the SSL protocol within the GEMS server is optional. The Florida team found then even when the SSL protocol was enabled security vulnerabilities still existed.

The Assure 1.2 software release does not address this issue. Premier Election Solutions believes that disabling the SSL protocol feature with the GEMS system is a security choice and advises customers to use the SSL features. Premier Election Solutions does not believe that their implementation of SSL is insufficient.

3.4 Other states using the Assure 1.2 platform

The Premier Election Solutions Assure 1.2 software release is currently certified for use in the state of Florida. Actual installation of the Assure 1.2 platform had not yet occurred at the time that this report was written.

All other customers of Premier Election Solutions require the same VSS certification as the State of Alaska in order to implement Assure 1.2. As such Assure 1.2 has not been installed on any known systems in the United States.

No known AccuVote systems have used the Assure 1.2 revision in a live election.

3.5 Division of Elections AccuVote Security Enhancements and Features Evaluation

The State of Alaska Division of Elections provided the UAA project team with a list of suggested security improvements during Phase 1. This list of enhancements and features is provided in "Appendix L – State of Alaska, Division of Elections Accu-Vote Security Enhancements and Features".

This section evaluates the DoE enhancements and features against the Assure 1.2 software revision enhancements. Cases where the issue identified by the DoE are resolved or mitigated by the Assure 1.2 software or firmware are presented in this section.

3.6.1 Verify GEMS Certified Software Has Not Been Altered

The Division of Elections desires to compute a hash code of the GEMS software to ensure that the currently running version has not been compromised.

The Assure 1.2 software release addresses this issue. Premier Election Solutions Premier's Windows Configuration Guide, Revision 3.0, Section 10 (2007) provides a detailed procedure for hash code validation of the GEMS software.

3.6.2 AV-OS / AV-TSX Supervisor Mode Password Changes

The Division of Elections desires to change the supervisor access passwords for the AV-OS and AV-TSX devices as regular intervals.

The Assure 1.2 platform in combination with the Keycard Tool application allows authorized users to change the supervisor access password for the AV-TSX device. The Assure 1.2 platform allows the authorized users to change the supervisor PIN for the AV-OS device.

3.6.3 AV-OS / AV-TSX Memory Card Wipe

The Division of Election desires to clear the memory of previous elections from all system memory cards prior to conduction of a new election.

The Assure 1.2 software release does not address this issue. Premier Election Solutions recommends using the AV-OS diagnostic menu to erase the contents of the AV-OS memory card. An external PCMCIA reader / writer is recommended for re-formatting the AV-TSX memory card units.

3.6.4 AV-TSX VVPAT Bar Code Removal

The Division of Elections desires to remove the time stamp bar code from the VVPAT printout.

The current software platform supports this feature.

4 Recommendations

It is the recommendation of the SOAESP project team that the State of Alaska, Division of Elections install the Assure 1.2 revision. Installation of this system revision is recommended for implementation following the 2008 election cycle.

Although the Assure 1.2 revision represents significant enhancements to system security two issues exist which make the installation of the Assure 1.2 revision impossible for the 2008 election cycle. Firstly, the Assure 1.2 revision software is not yet certified to the Voting System Standards (VSS) 2002 specification. The Assure 1.2 revision is currently in review with the nationally recognized testing agency SysTest. Formal certification from this agency has not yet been received by Premier Election Solutions and is required by Alaska State Law for installation on Division of Elections hardware. Secondly, the Division of Elections resources for the 2008 election cycle are not sufficient to complete the upgrade prior to the primary election which takes place in August, 2008.

It is recommended that the Assure 1.2 revision be implemented by the Division of Elections following the general election in 2008 and is contingent upon Premier Election Solutions receiving formal certification from SysTest.

Appendix C - Assure 1.2 Upgrade Issue Resolution Matrix

SOAESP Issue Number	Reference Document	Reference Document Section	Issue Description	Assure 1.2 Status
3.2.1	California Red Team Review	Section 3	Precinct Count AV-OS Ballot Tampering	Corrected by adding counter integrity checking with public counter
3.2.2	California Red Team Review	Section 4b	AV-TSX Malware	Corrected bootloader issue, Premier rejects format string error vulnerability
3.2.3	California Red Team Review	Section 4c	AV-TSX Escalation of Privileges	Corrected - can still enter system setup/diagnostics when peripheral device fails but cannot access administrative functions.
3.2.4	California Red Team Review	Section 4d	AV-TSX Default Static Key	No change, Premier believes default key indication is a feature.
3.2.5	California Red Team Review	Section 1b	GEMS Databases	Corrected - improved database security, corruption of database file (as compared to modification) by system administrator cannot be prevented since, by definition, the system administrator has full system access.
3.2.6	California Red Team Review	Section 1c	GEMS Audit Logs	The database is password protected in Assure 1.2. However, standard security practices with the GEMS server are critical.
3.3.1	Florida Analysis	Section 3.5	RSA signature flaw.	Corrected in Assure 1.2
3.3.2	Florida Analysis	Section 3.6	AV-OS Memory Card Integrity Is Not Protected	Complete authentication is beyond the capability of the AVOS hardware. While some improvements have been made, for example protecting the Abasic report scripts, physical protection of the memory card contains to play a critical role.
3.3.3	Florida Analysis	Section 3.7.1.1	AV-TSX Cryptographic Key Management	Premier recommends that all AV-TSX systems utilize the Keycard Tool Application
3.3.4	Florida Analysis	Section 3.7.1.2	AV-TSX Memory Card Update File is Unprotected	Corrected
3.3.5	Florida Analysis	Section 3.7.1.3	AV-TSX Smart Card Authentication Uses Only a Hard Coded Password	No change. The smart card does not use hard coded passwords. The issue was the authentication method used by the smart cards. This is mitigated procedurally by poll workers' monitoring for suspicious activity with smart cards or voters spending excessive time at the machine
3.3.6	Florida Analysis	Section 3.7.1.4	AV-TSX Supervisor PIN is Not Cryptographically Protected	No change. The issue is that the reviewer did not consider the protection robust enough rather than there not being any protected. Mitigated procedurally by restricting access to supervisor cards.
3.3.7	Florida Analysis	Section 3.7.1.5	AV-TSX Insecure Storage Mount	Corrected
3.3.8	Florida Analysis	Section 3.7.1.6	AV-TSX System Configuration is Unprotected	No Change - this is not a vulnerability since there is no ability to externally access this data.
3.3.9	Florida Analysis	Section 3.7.1.8	AV-TSX Ballot Definition File is Unprotected	Corrected - The file was actually protected but the reviewer considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.10	Florida Analysis	Section 3.7.1.10	AV-TSX No Integrity Protection of Stored Electronic Ballots	Corrected - The file was actually protected but the reviewer considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.11	Florida Analysis	Section 3.7.1.11	AV-TSX Ballots are Stored Sequentially	Exploiting this requires access to encryption keys of which there is no external ability to access.
3.3.12	Florida Analysis	Section 3.7.1.12	AV-TSX Candidate Information is Not Stored in the Results File	Premier disagrees that this is a security problem. No change
3.3.13	Florida Analysis	Section 3.7.1.13	AV-TSX Audit Logs Are Not Cryptographically Protected	Corrected - The file was actually protected but the FS review considered the protection to be too weak. Have changed to using a SHA1 HMAC
3.3.14	Florida Analysis	Section 3.7.1.14	AV-TSX Data is Neither Authenticated Nor Encrypted Over the Communication Link	Corrected - The issue was not that the data was not encrypted but that the seed used to initialize the encryption system did not contain enough entropy.
3.3.15	Florida Analysis	Section 3.7.2.1	AV-TSX Bootloader Automatically Replaces Itself	Corrected - Updating the bootloader now requires authentication of the operator and the new bootloader.
3.3.16	Florida Analysis	Section 3.7.2.2	AV-TSX Bootloader Automatically Replaces Operating System	Corrected - Updating the Operating System now requires authentication of the operator and the new Operating System
3.3.17	Florida Analysis	Section 3.7.2.3	AV-TSX Bootloader Automatically Runs .ins Files on the Memory Card	Corrected - Running an .INS file now requires authentication of the operator and the .INS file.
3.3.18	Florida Analysis	Section 3.8.1.1	AV-OS Leaks Memory Card Contents	Access to this capability is limited by locking the AVOS onto the ballot box and by locking the cover to the yes/no keys.
3.3.19	Florida Analysis	Section 3.8.1.2	AV-OS Supervisor PIN Not Cryptographically Protected	Due to hardware limitations, there is no secure storage for the PIN. Thus procedural mitigation is required, as it has been in the past.
3.3.20	Florida Analysis	Section 3.8.1.3	AV-OS No Authentication Between GEMS and the Terminal	This upload is for unofficial results only. The upload at election central occurs in a secure environment.
3.3.21	Florida Analysis	Section 3.8.1.4	AV-OS Attacker Can Hide Pre-loaded Votes	Corrrected
3.3.22	Florida Analysis	Section 3.8.1.5	AV-OS Vote Counters Are Not Directly Checked for Overflow	Corrected
3.3.23.1	Florida Analysis	Section 3.9.1	Error Checking Is Inadequate in AccuBasic	No Change The report failed to demonstrate any security risk.
3.3.23.2	Florida Analysis	Section 3.9.2	Error Codes Returned by the AV-OS System are Ignored	No Change The report failed to demonstrate any security risk.
3.3.23.3	Florida Analysis	Section 3.9.5	AccuBasic Unchecked String Operation	Corrected
3.3.24	Florida Analysis	Section 3.10.1	GEMS AccuBasic Scripts are Not Authenticated On the GEMS Server	No change. The scripts are authenticated on the AV-OS and AV TSx, not on the GEMS server
3.3.25	Florida Analysis	Section 3.10.2	GEMS Password Does Not Protect Access to GEMS or Audit Logs	The database is password protected in Assure 1.2

3.3.26	Florida Analysis	Section 3.10.3	GEMS Incomplete Implementation of the SSL Protocol	Disabling this feature is optional. Policy should be to enable this feature.
3.6.1	State of Alaska Division of Elections	GEMS Item 1	Verify GEMS Certified Software Has Not Been Altered	Hash code validation procedures for software installed on GEMS servers are documented in section 10 of *Premier's Windows Configuration Guide Rev 3.0*.
3.6.2	State of Alaska Division of Elections	Memory Card Item 6	AV-OS / AV-TSX Supervisor Mode Password Changes	Use of the Keycard Tool application allows password changes on AV-TSX. Authorized Users may change the Supervisor PIN on the AV-OS platform
3.6.3	State of Alaska Division of Elections	Memory Card Item 9	AV-OS / AV-TSX Memory Card Wipe	While Premier does not offer a wipe utility *per se*, AVOS memory cards may be erased in diagnostic mode on the AVOS. TSx memory cards may be reformatted in a non-network-connected, known secure computer with a PCMCIA card reader.
3.6.4	State of Alaska Division of Elections	Voting Equipment Item 2	AV-TSX VVPAT Bar Code Removal	System is capable of bar code removal

Appendix D - Division of Elections Enhancement Analysis

1. Introduction

This document evaluates the State of Alaska, Division of Elections AccuVote Security Enhancements and Features (2007) document to determine whether the proposed changes to the system are feasible in the currently implemented system.

Each suggested enhancement or feature listed in this document is presented as shown in the State of Alaska, Division of Elections AccuVote Security Enhancements and Features (2007) document and is followed by a discussion and recommendation regarding that enhancement or feature.

2. Enhancement / Feature List

2.1 Software Hash Validation

Description

Verify the certified software installed has not been altered by computing the digital signatures of the software and comparing them with the digital signatures of the certified version.

The digital signature comparison should be performed at least:

a. Immediately after installing a new component or new version of software.
b. After any unusual or suspicious event.
c. Before beginning the set-up of a new election.
d. Immediately after completing an election.

Comments / Recommendation

Calculation of the digital software signature for the components operating on the GEMS server and on personal computer based software components or applications (Key Card Tool, VC Programmer) is recommended. The suggested hash validation plan presented by the Division of Elections is reasonable. Although hash validation of the EPROM chips present in the AV-OS machines is possible the logistics associated with removal and validation of the EPROM chips prior to each election cycle is significant. As such we recommend validating hash codes on AV-OS machines only on an individual case by case basis in circumstances where an unusual or suspicious event has occurred. We also recommend the use of tamper evident markers on the EPROM chips as well as marking each EPROM chip with a unique serial number to increase the confidence in the AV-OS firmware and lessen the requirement for periodic hash code validation of the AV-OS firmware.

2.2 GEMS Network Access and Exclusive Use

Description

Ensure that no GEMS computer is connected to a network or the internet and do not allow any software on the GEMS computer except for the voting system software itself. Use only the GEMS computer for programming an election.

Comments / Recommendation

It is crucial to the security of the GEMS servers that local network and internet connectivity be avoided. As such careful attention must be paid not only to ensuring that connectivity does not exist but also to ensuring that connectivity would be difficult or impossible to achieve by malicious users. The GEMS server should not be housed in close proximity to other network access equipment including packet communications switches, routers, etc. Premier Election Solutions Premier's Windows Configuration Guide (2007) provides detailed configuration information regarding the acceptable configuration of GEMS servers to be used in an AccuVote system. It is recommended that the Division of Elections follow these guidelines. The GEMS server should be exclusively used for the purpose of programming elections and for no other purpose (specifically it is recommended that any implementation of the Key Card Tool application be performed on a separate personal computer platform dedicated to that purpose).

2.3 Authorized GEMS Access Restriction

Description

Restrict access to the voting system to authorized personnel only and maintain an access log to record each time a person accesses the GEMS computers.

Comments / Recommendation

Maintaining a secure system by limiting access only to authorized personnel is recommended. Authorization to obtain access to the GEMS system should be based on individuals completing security training. This security training should familiarize the user with standard security procedures for use with personal computers, the Windows operating system and the GEMS software specifically. The use of access logs is not a recommended enhancement given the small number of system users (see "Appendix E – Physical Password Management Recommendations", Section 2 Recommendation 2).

2.4 Election Program Control

Description

Do not allow any changes to the election program once the logic and accuracy testing has commenced.

Comments / Recommendation

Knowledge of the election program status at all times in the election process is recommended. The Division of Elections current implementation of locking the election program once logic and accuracy testing has begun is recommended to ensure consistency and validity of the test results.

2.5 Voting System Access Control

Description

Never allow vendor personnel to access the voting system unless an authorized member of election staff is present.

Comments / Recommendation

Supervision of all non-staff individuals requiring access to the election system is recommended. Vendor supervision is strongly recommended.

2.6 Password Management Policy

Description

Establish policy for password management. Change passwords on a periodic basis and at least once an election cycle or once a year.

Comments / Recommendation

Management of the passwords utilized with the Division of Elections AccuVote system is crucial to implementing a secure, reliable election system. We recommend following the password management guidelines presented in the attached "Appendix E - Physical Security and Password Management Recommendations". This document outlines a password management strategy which incorporates the challenges faced by election officials working in the State of Alaska.

2.7 Background Checks

Description

Perform background checks on staff authorized to:

a. Define and configure elections
b. Maintain voting equipment
c. Enter election results into GEMS
d. Gain access to voting system or system components

Comments / Recommendation

We recommend requiring background checks on new employees (authorized to perform tasks list above) in accordance with state and labor union regulations.

2.8 Director's Office Memory Card Storage

Description

Memory cards stored in the director's office are to be maintained in a secured environment.

Comments / Recommendation

Secure storage of the AccuVote memory cards is strongly recommended. Physical access security precautions outlined in "Appendix E - Physical Security and Password Management Recommendations" are recommended to be used for secure all election components deemed vulnerable to malicious attack.

2.9 Memory Card Chain of Custody

Description

Memory cards, once programmed and tested, that are shipped to the regional offices need to be shipped using chain-of-custody security measures.

Comments / Recommendation
We recommend using a shipper (such as DHL, FedEx, Alaska Airlines Gold Streak) with chain of custody processes to transport memory cards to regional offices prior to elections.

2.10Regional Office Memory Card Storage

Description

Once memory cards are received in regional offices they are to be maintained in a secured environment.

Comments / Recommendation

Secure storage of the AccuVote memory cards is strongly recommended. Physical access security precautions outlined in "Appendix E - Physical Security and Password Management Recommendations" are recommended to be used for secure all election components deemed vulnerable to malicious attack.

2.11Memory Card Tracking Audit Capability

Description

Have audit / receipt tracking form to compare against sent memory cards and received memory cards that is signed off.

Comments / Recommendation

The ability to track and account for all memory cards system-wide is highly recommended. We recommend implementing a bar-code inventory process next year (after elections) and including memory cards in the inventory.

2.12Memory Card Pre-election Tamper Security

Description

Send memory cards to election board in tamper-sealed envelopes for insertion into the units on election morning. Require election board to verify envelope is sealed prior to opening and sealing memory card in voting unit. Since equipment is in the possession of the election chairperson prior to election day, keeping the memory cards sealed until election morning removes the possibility of tampering with the memory card by the person with possession.

Comments / Recommendation
We agree that that Division should ship memory cards in tamper evident envelopes and that the election board verifies the integrity of the seals and insertion of the cards into machines (if the memory card hasn't already been installed in the voting machine).

2.13Supervisor Mode Password Change

Description

Consider password changes to access supervisor mode.

Comments / Recommendation

It is highly recommended that the password utilized to access supervisor mode be changed at a minimum once per election cycle and that the distribution of the supervisor password be strictly limited to election officials requiring supervisor access only.

2.14Memory Card Inventory Accounting

Description

Maintain inventory log and accountability of all memory cards with election programming to ensure all cards are returned after the election.

Comments / Recommendation

It is recommended that the measures recommended in section 2.11 be used to confirm the receipt of all returned memory cards used during an election cycle.

2.15Battery Replacement Schedule

Description

Establish a timeline for battery replacement of memory cards.

Comments / Recommendation

Premier Election Systems documentation specifies memory card battery life at 5 years. It is recommended that the Division of Election replace AV-OS memory card batteries every other election cycle or when the memory card battery life indicator shows a low battery. Documentation of the battery replacement plan should be developed to ensure that historical battery replacement chronology can be produced as need.

2.16Previous Election Memory Card Wipe

Description

Establish a timeline of previous elections information to be removed from memory cards.

Comments / Recommendation

It is recommended that the contents of each memory card be cleared prior to each election (primary and general).

2.17AV-TSX VVPAT Flap Removal

Description

Remove the flap from the VVPAT viewing location so voters know they can review the paper version of their ballot.

Comments / Recommendation

It is recommended that the VVPAT flap on the AV-TSX machine be modified to include a label which instructs the voter to lift the VVPAT flap to review the voted ballot. This implementation retains voter privacy while ensuring that the voter is aware of the ballot review feature.

2.18AV-TSX Bar Code Removal

Description

Remove the bar code from the VVPAT ballot.

Comments / Recommendation

It is recommended that the bar code printed on the AV-TSX VVPAT ballot be deactivated in the BallotStation software to lessen the probability of voter identification after using the AV-TSX machine and increase voter anonymity.

2.19AV-TSX Use Encouragement

Description

Encourage at least 5 votes cast on the touch screen as a means of protecting voter privacy with the use of the reel-to-reel printer.

Comments / Recommendation

It is recommended that precinct officials encourage voters to use the AV-TSX machines as much as possible to reduce the risk of voter privacy violations. A minimum of 5 votes should be considered the absolute minimum vote count required for the AV-TSX and more votes should be encouraged.

2.20 Voting Machine Tracking and Accounting

Description

Maintain record of the serial number of each voting unit and which precinct the unit was sent to.

Comments / Recommendation

It is recommended that the serial number, firmware / software versions and functional test results from each election cycle along with the destination precinct be recorded and maintained in electronic historical archives.

2.21 Physical Security Review

Description

Conduct a physical security review to assess the access and control procedures for areas where voting equipment and components are stored and maintained. Establish policy for access to area where equipment is stored, including the restriction of vendor and non-election employees to have uncontrolled access.

Comments / Recommendation

We recommend that the physical security recommendations outlined in "Appendix E – Physical Password Management Recommendations" be implemented in the 2008 election cycle. We further recommend that the Division of Elections conduct a physical security review using a professional security agency at each location where voting equipment is stored.

2.22 Asset Management Plan

Description

Implement asset management and inventory control system for voting equipment and components, including the software and firmware installed on each piece of voting equipment.

Comments / Recommendation

It is recommended that the functional testing, voting machine tracking and accounting (section 2.20) and the asset management plans be incorporated into a single procedure in which a complete documentation package is produced for each voting machine during each election cycle. The contents of the documentation package should be scanned into electronic format for long term archival storage.

2.23 Tamper Evident Seals

Description

Implement the use of tamper-evident seals.

Comments / Recommendation

We recommend that the Division of Elections use tamper-evident seals on AV-OS and AV-TSX machines. Section 1.6 of the main document includes a detailed description of this recommendation

2.24Vendor Repair Acceptance Testing

Description

Implement testing procedures and sign-off on all equipment returned from vendor after maintenance and / or repair to ensure proper versions of the hardware, software and firmware.

Comments / Recommendation

It is recommended that acceptance testing and documentation be performed prior to accepting equipment returned from the vendor for repair or maintenance. The acceptance test procedure should follow the tests outlined in "Appendix M - AccuVote Functional Test Guidelines". Documentation confirming that the returned machine passed the required tests should be produced and stored electronically in the historical archive.

2.25AV-TSX Inter-election Storage

Description

Consider process for the storage of touch screen voting units in remote areas of the state between the Primary and General elections.

Comments / Recommendation

We recommend storing touch screen voting units in locked closets or cabinets between elections. However, the machines take up a lot of space, and this may not be possible. In which case we recommend storing them in a lockable facility.

2.26Functional Test Guidelines

Description

Establish functionality testing schedule and procedures for all voting equipment.

Comments / Recommendation

It is recommended that the Division of Elections adopt the functional test guidelines presented in "Appendix M - AccuVote Functional Test Guidelines". This document outlines a suite of tests and provides recommended documentation guidelines for use with the AccuVote system in the State of Alaska.

2.27Logic and Accuracy Test Improvements

Description

Update logic and accuracy testing reports for voting equipment based on where equipment is used, polling places, early voting ballot counting at regional offices.

Comments / Recommendation

It is recommended that the Division of Elections adopt the logic and accuracy improvements and enhancements outlined in “Appendix N - AccuVote Logic and Accuracy Test Guidelines”. This document details a suite of logic and accuracy tests and documentation guidelines to help ensure tabulation accuracy and election programming validity.

2.28Post Election Audit Validation

Description

In post-election audit, compare all election results transmitted via modem from the polling place against the actual results printed by the election board prior to transmission.

Comments / Recommendation

It is recommended that the transmitted results be compared with the printed results to confirm accuracy. Inconsistencies between the transmitted results and the printed results must be documented and resolved prior to official results being released by the Division of Elections.

2.29Central Administrator Card Controls

Description

Establish inventory controls and procedures for the security of the Central Administrator Cards for touch screen voting system.

Comments / Recommendation

It is recommended that the AV-TSX Central Administrator cards be secured in the highest security area and passwords associated with the Central Administrator card be given only to authorized individuals requiring Central Administrator access.

2.30Security Standards for Loaned Voting Machines

Description

Establish basic security standards of voting equipment that is used or stored by city / borough entities.

Comments / Recommendation

It is recommended that entities utilizing State of Alaska owned voting machines should be trained regarding election system security and the policies adopted by the State of Alaska. Complete functional testing of loaned voting machines should be performed upon return of the voting machines to the Division of Elections. Documentation of these tests should be produced and archived.

2.31Municipal Owned Machine Use Policy Review

Description

Consider policy on the use of municipal owned voting equipment being used in state and federal elections. There is a location in the state where the municipality owns the optical scan and the state uses it during elections.

Comments / Recommendation

It is recommended that the State of Alaska procure enough machines to service all precincts required and that the State of Alaska not utilize machines owned and stored by other government entities.

Appendix E - Physical Security and Password Management Recommendations for GEMS Servers

1. System Overview

This document describes the existing safeguards employed by the State of Alaska, Division of Elections to protect the Global Election Management System (GEMS) hub and regional servers. The discussion is limited to the physical security and the password mechanisms in place that relate to the GEMS servers. Related topics, such as recommended Windows configurations, disaster planning, or malware prevention are not discussed here.

The security mechanisms consist of the physical building security and three layers of password-protected systems: BIOS (Built-In Operating System) password, Windows authentication, and GEMS Database server authentication. These mechanisms are depicted in Figure 1.

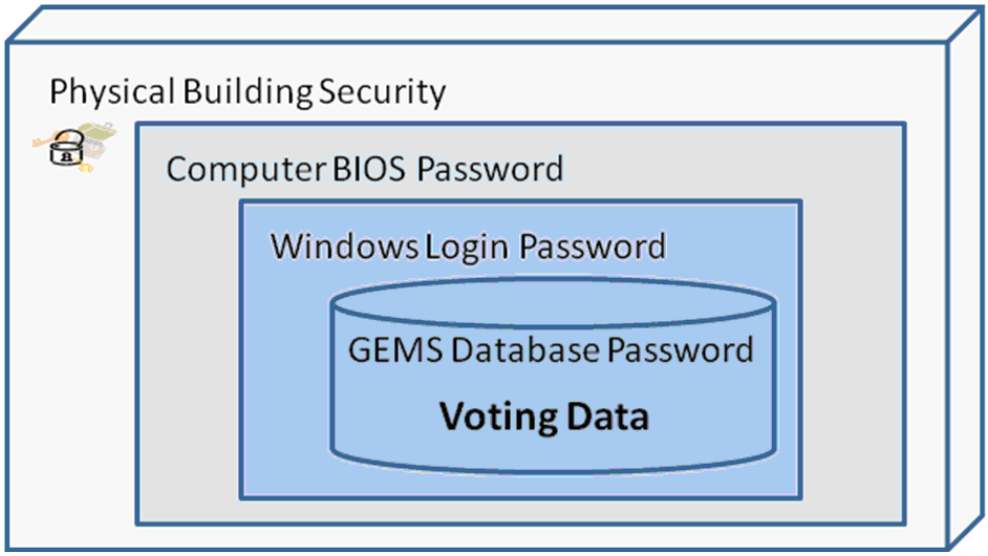


Figure 1. Layers of protection afforded by passwords and physical security

1.1 Existing Physical Security

The Division of Elections maintains eight GEMS servers, two host servers for Director's Office use (one is a backup), one for Region I (handcount use), one for Region II (handcount use), two for Region III (multiple servers for handcount efficiency), two in Region IV (multiple servers for handcount efficiency). The host server is used to program the databases for dissemination to the regional GEMS server prior to an election and for aggregating results from the regional GEMS servers after an election. Several regional supervisors reported that the regional GEMS servers are not frequently used – they are primarily used to hand-enter election results from hand-count precincts and for hand-count results entry in precincts where the AV-OS upload has failed.

The host server is administered by the GEMS programmer. The GEMS programmer also sets accounts and passwords for the regional servers that are operated by the regional Election Supervisors. The physical security varies by location, but it is the Division of Election's policy to keep all GEMS servers, voting equipment, and components of the voting systems (e.g. memory cards) in a locked and/or alarmed room.

- Host server: Juneau

  The host server is located in a locked, alarmed room. Three employees have access to the room. The door is unlocked by a key that is stored in a private desk drawer.

- Region I: Southeast

  The GEMS server is located in a locked, alarmed room. The election equipment is located in a separate locked room that can be alarmed. Two employees have access to the rooms.

- Region II: Anchorage and Matanuska Valley

  The GEMS server is located in a locked, alarmed room together with the touch screen units. The optical scan units are stored in an outer room, also locked and alarmed. Three employees have access to the GEMS server room. An additional key is available to staff, but only the three employees know the alarm access code.

- Region III: Fairbanks and Interior

  The GEMS server is located in a locked room. Three employees have access to the server room. Unlike the other regions, activity in this room is high since a staff member has a desk located in the room.

- Region IV: Nome, Barrow and West Coast

  The GEMS server is located in a locked back conference room. Two employees have access to the room which also stores other election equipment.

Access to the rooms is limited to authorized Division of Elections employees. All non-employees entering the room must be accompanied by an authorized Division of Elections employee. Division employees go in and out of the rooms frequently and do not maintain an entry or exit log.

1.2 Existing Password Management Policies

Systems that may be secured by password include alarm access codes, BIOS passwords, Windows login passwords, and GEMS database passwords.

Alarm access codes consist of a numeric PIN and are used to enable or disable the alarm system, if one exists.

A BIOS password requires the user to enter a password to boot the system. This may be enabled in the BIOS for the GEMS servers. Only a single password is stored; i.e. there is

no per-user authentication. The password is stored in flash memory or refreshed by an internal battery. None of the Division of Elections supervisors reported that a BIOS password was enabled on their server.

Windows login passwords are used to log into the GEMS servers, which are currently running a version of Windows 2000. There is only one account for each server and users share accounts. For example, there is a generic user account used by two different users to log in for a given GEMS server. The number of users sharing an account is never more than three and is typically a single user. Regional supervisors were unsure about details of account policies, including password aging (a mandatory change to a new password after some time period has elapsed), number of re-tries if an invalid password is entered, and password generation details. The regional supervisors indicated that the account policies should be identical to the host server, which reportedly locks out users after three failed attempts and implements password changes every election cycle. However, one regional administrator reported that the Windows password had not been changed, indicating that mandatory password aging has not been implemented in all cases.

The GEMS database stored on each GEMS server is further protected by a database-level password. Prior to every election the GEMS host programmer sends the election database to the regional supervisors. The database is sent physically on a CD and shipped via a tracked shipping method. Access to the database requires a username and password which is set in the master database at the time of creation. The username and password are changed once every election cycle. The usernames and passwords are selected and discussed during the senior manager's conference call and typically consists of a phrase with mixed case letters and numeric characters. The usernames and passwords are shared with the regional supervisors via telephone call. The process is illustrated in Figure 2.

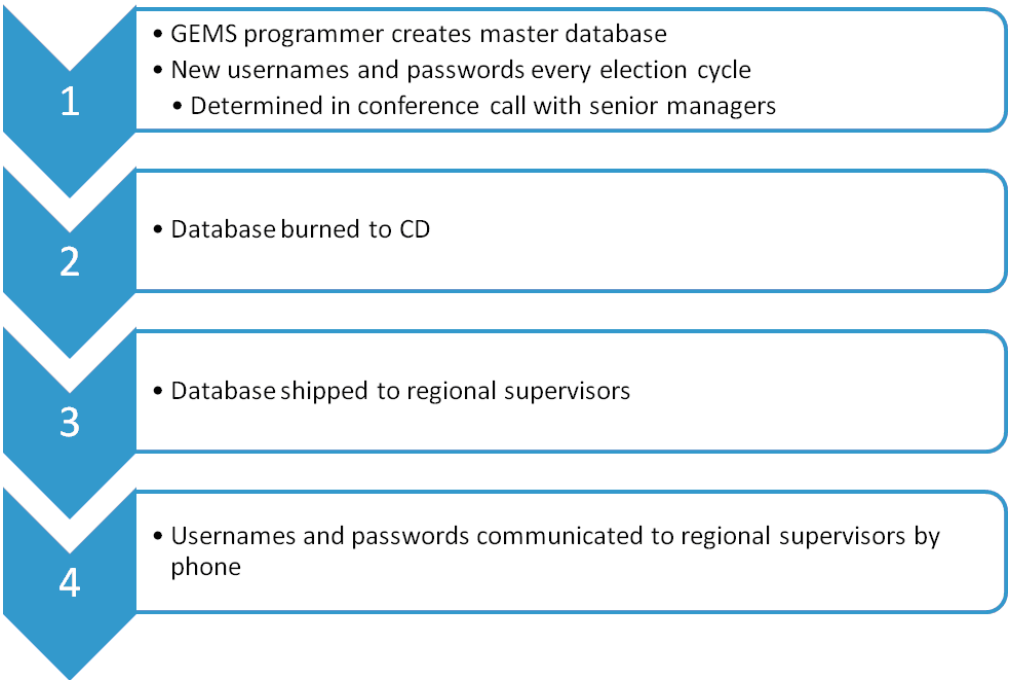


Figure 2. Distribution mechanism for GEMS database usernames and passwords

At the time of this report, there are seven usernames and passwords. The database username and password is always different from the Windows login username and

password, although in most cases when a user logs in on the same regional GEMS server they will use the same Windows login and the same database login.

2. Physical Security Recommendations

In the GEMS system, physical security arguably presents the greatest opportunity to deter malicious attack. Given unfettered access and sufficient time a determined attacker will likely be able to circumvent the BIOS, Windows, and database passwords. Removing physical (and remote) access eliminates many avenues of attack.

Our recommendations for physical security are similar to many of Premier's recommendations described in the Client Security Policy documentation (Diebold Election Systems, 2007) but have been adjusted for the Division of Elections work environment.

Our recommendations are to:

1. Fortify the structure enclosing the GEMS server and associated infrastructure so it may not easily be entered by force.

2. Do not maintain entry and exit logs to the GEMS server rooms. This is not practical given the high volume of access in several locations, primarily by the same employees. We recommend continuing the practice of requiring an authorized Division employee to be in the room at all times to supervise any non-authorized persons are in the room.

3. At a minimum, continue to secure the GEMS server and associated infrastructure in a locked room. We also strongly recommend a monitored alarm system. Other considerations include a video surveillance system, fireproof door, temperature controls to maintain the temperature between 50-80 degrees Fahrenheit, and a two-factor entry system. Two-factor authentication requires two methods to enter the room (e.g. key and biometric fingerprint scanner, key and alarm passcode, etc.)

4. Where feasible the GEMS server and associated infrastructure should NOT be stored in the same room as other election equipment (e.g. touch screen or optical scan units) to physically separate those personnel authorized to access the other election equipment but not the GEMS server.

   In instances where it is not feasible to physically separate the GEMS server from other election equipment the equipment storage area should be used exclusively for storage. All testing, tabulation, validation and other process related activities should be performed in a workspace separate from the GEMS storage area. Access to the GEMS servers should be carefully monitoring and limited to authorized personnel only.

5. All doors should be locked when the equipment is not in use.

6. Practice the principle of least access. Access to the GEMS server room should be kept to the minimum number of privileged personnel.

7. Establish a procedure to regularly inspect and maintain physical locks and test alarm systems.

8. Keys to the GEMS server room should not be left in a location accessible to non-authorized personnel (such as cabinets or drawers). Authorized personnel should carry a key on their person or store it in a securely locked location, such as a safe. Any non-authorized personnel wishing to enter the room must have an authorized employee open the door and monitor the non-authorized personnel's activity while in the room.

9. The server should have a locked bezel to deter disk bays from being accessed or the cover from being opened.

10. Establish a written, formal physical security policy that addresses the above considerations and includes policies to change access codes or keys when employees leave, backup and recovery procedures, backup power, fire emergency plan, and procedures to periodically review existing or new physical security controls. These procedures should assess known risks and identify vulnerabilities associated with the physical environment. This periodic review is necessary because appropriate policies and procedures may need revision as technology changes over time, or vice versa.

3. Password Management Recommendations

Passwords provide a secondary line of defense if physical security is compromised. We recommend employing BIOS passwords as an additional security control on top of the Windows and GEMS database passwords. All passwords should be "strong" in the sense that they are not easily guessed or determined through systematic means.

An example of a weak password is any word found in a dictionary. An attacker could determine the password by brute force, trying every word in the dictionary (automated by a program) until the password is found. Another weak password is one that is too short or selected from a small set of characters. Consider a 4-character password comprised of lowercase letters. This allows $(26)^4$ or 456,976 possible passwords. A brute force program could easily enumerate all possibilities and quickly determine the password. However, if the set of characters is expanded to include uppercase letters and digits, and the length is increased to 8, then the number of passwords becomes $(62)^8$ or 2.2×10^{14}, a much larger number that makes the password more difficult to guess or determine through brute force.

However, we must recognize that strong passwords alone do not guarantee protection. For example, an attacker could bypass the Windows login password by physically removing the hard drive and mounting it on a separate system to examine its contents. Similarly, the strongest passwords are useless if an unauthorized observer "shoulder surfs" by watching the keys pressed by an authorized user as she enters her password, or if the passwords are discovered by an attacker on a written piece of paper. Moreover, in the case of the GEMS servers, the security of the underlying operating system is much easier to break than the password security. As one example, the RABA report (RABA Technologies LLC, January 20, 2004) describes how to exploit a Windows bug on an unpatched GEMS server to gain administrator access by merely dialing into the system's modem with a software product called Canvas. Additional defensive controls must be in place to secure the system and the passwords themselves to mitigate potential attack.

3.1 Tradeoffs between usability and password strength

While longer and more complex passwords increase the cryptographic strength, a tradeoff must be made with usability, i.e. the ease of which users are able to work with the system. For example:

- Long and complex passwords are hard to remember.
- If a password is hard to remember then it is more likely to be written down, providing an attacker easy access if the written password is discovered.
- If a user has to remember many passwords then it is more likely they will be written down, providing an attacker easy access if the written passwords are discovered.

A balance must be made between password length, number, and memorability. We recommend the following criteria for password selection and storage:

1. Passwords should be at least 8 characters and include mixed-case, at least one digit, and at least one non-alphanumeric character.
2. Ideally, passwords should not be written down or the risk of disclosure will increase. If they must be written down then the password must be stored in a secure, non-obvious location that is not in the same room as the server. For example, we do not recommend storing the password in a desk (even if locked) in the server room or in the desk of the employee that commonly frequents or manages the server room. A safe would constitute a secure location.
3. Optionally, to increase the memorability of passwords, several techniques are possible, such as concatenating the first few letters of words in a phrase while inserting digits or non-alphanumeric characters. For example, if the phrase is "**sec**ure **ele**ctions **eve**ry **tim**e" then the password could be **sec**4**ele**+**eve**&**Tim**. Recent research indicates that using such mnemonic passwords schemes still leaves the system vulnerable to smart-dictionary types of attacks (Kuo, Romanosky, & Cranor, 2006), although the vulnerability is likely to be exploited only in the more distant future
4. The same password should never be used in a different system. For example, the BIOS password should not match the GEMS password. Similarly, the Windows password should not match an employee's personal Google password.

A related and sometimes contentious issue is password aging, or the practice of forcing users to change their passwords after a certain number of days has elapsed. A password history can also be kept so users cannot revert to a previous password.

The major benefit of password aging is to safeguard against guessing and unknown disclosure. For example, if a password has not been changed for years but has been leaked unbeknownst to the owner, perhaps through accidental disclosure, then regular password changes will prevent an unauthorized user from logging in. We include "unbeknownst to the owner" because if the leak is known then the password should be changed immediately and the machine examined for tampering.

Conventional wisdom and the Diebold Client Security Policy (Diebold Election Systems, January 11, 2007) suggest a password age no more than 45 days and a history of 10 passwords. However, the benefits of password aging are fairly modest and can actually be destructive (Spafford, 2006):

- Password changes offer no protection against password snooping and operating system level attacks.

- Frequent password changes make the password harder to remember and becomes more likely to be written down, increasing the potential for disclosure.

- To generate a new and memorable password that is not in the history list, many users use an algorithm that can be easily guessed, such as appending a different digit onto the end of the password. This practice also increases the potential for guessing if old passwords are disclosed.

- If a password has been obtained by an attacker then the mandatory password change is likely weeks away, giving the attacker many days to authenticate and attack the system. This scenario can be mitigated by incorporating additional security controls that the attacker must also confront. For example, if an attacker discovers the password but doesn't yet have a way to get into the room then password aging will thwart the attacker if the password is changed before the attacker finds a way to gain physical access.

Due to the relatively modest gains of password aging and the negative impact on memorability we suggest a less aggressive aging schedule than the Diebold recommendations. Specific recommendations relating to password aging are given in the following sections. Our recommendations regarding password management have also been targeted specifically for the Alaska Division of Elections GEMS environment. For example, with less than 10 users and infrequently used servers, the same policies are not always appropriate that would be used in the common IT scenario involved in authenticating hundreds of users on an enterprise network.

3.2 BIOS Password

A BIOS password prevents the system from booting if an incorrect password is entered. This prevents several trivial attacks, such as booting up from a floppy disk to run a program that extracts the Windows administrator password, to booting from an external hard drive to run a program that examines the internal hard drive. However, with enough time and access an attacker can easily bypass a BIOS password. The BIOS password can typically be reset by removing the internal battery or reconfiguring jumpers on the motherboard. This is one reason why the computer's case should be physically locked (recommendation 2.9). Some BIOS's also have known, hard-coded passwords.

We recommend:

1. All GEMS servers should incorporate a BIOS password conforming to the password selection and storage criteria described in section 3.1.

2. The BIOS should be configured to boot from the hard drive only.

3. The BIOS password should be changed anytime an authorized employee leaves the organization or disclosure is suspected.

4. Since there is only one BIOS password it must be shared among all authorized personnel that use the system. The password should not be shared with anyone else.

3.3 Windows Passwords

The next line of defense is the Windows logon password. As previously discussed, there are many weaknesses in the Windows OS that a knowledgeable attacker may exploit to gain administrator access to the machine. Consequently, the Windows OS should not be considered secure, especially if it has not been patched. Nevertheless, Windows passwords do afford some level of protection, particularly against less technical malicious insiders.

We recommend the following policies and controls for the Windows login account of the GEMS server:

1. All GEMS servers should incorporate a Windows password conforming to the password selection and storage criteria described in section 3.1.

2. Lock out the user account after three consecutive failed login attempts. This can be configured as a security policy in Windows.

3. All users should have their own login account. Users should never share accounts. Passwords must never be shared with anyone, not even a system administrator. These same recommendations are made by Diebold (Diebold Election Systems, January 11, 2007).

4. All users should change their password at least once every election cycle. This could be implemented with a yearly aging policy with a password history of 5.

5. An authorized user should never leave the server unattended after logging in. If possible, the machine should be powered off when all authorized employees leave the room.

6. Consider two-factor authentication (e.g. biometric fingerprint scanner in addition to a typed password).

3.4 GEMS Passwords

The GEMS database requires authentication with a username and password before the database may be accessed. Similar to the situation with Windows passwords, the GEMS database should not be considered secure even if an attacker does not have a valid GEMS username and password. The GEMS server is based on Microsoft Access, and many techniques exist in the public domain to exploit and manipulate the contents of an Access database. Nevertheless, GEMS database passwords do afford some level of protection, particularly against less technical malicious insiders.

We recommend the following policies and controls for the GEMS database passwords:

1. The database passwords should conform to the password selection and storage criteria described in section 3.1.

2. All users should have their own database account. Users should never share accounts. Passwords must never be shared with anyone, except when disseminated by the GEMS programmer to the GEMS regional supervisor that will use that account.

3. The practice of changing passwords every election cycle is adequate, given the relatively low frequency of use. However, care should be taken in the way that the GEMS databases are disseminated via CD-ROM. If an attacker intercepts the CD-ROM during transit it may be possible to incorporate malicious software with the contents of the database onto a new CD-ROM and then forward the compromised CD-ROM to the regional supervisor. If the compromised CD-ROM is inserted into the GEMS server then the server may be compromised.

   To mitigate this possibility we recommend that either:

   1. The databases be hand-delivered to the recipients.

      or

   2. A hash/checksum tool be run on the CD containing the database to be transmitted. The checksum would be communicated to the recipient by phone. When the recipient receives the CD-ROM it would be tested on a third machine to verify that the checksums match before inserting the CD-ROM on the GEMS server.

3.5 Other Recommendations

We also recommend the following practices and procedures that are related to password security:

1. If the physical security of a GEMS server has been compromised, password management is only a secondary concern. The Windows operating system is the weakest link due to the numerous security flaws that have been well documented and publicized. Many tools are readily available that allow attackers to quickly gain administrator privileges using known security flaws. To protect against many of these attacks, the GEMS servers should be patched with the latest Microsoft security updates. Use the procedure described in the Diebold Client Security document (Diebold Election Systems, January 11, 2007), section 4.1.1. This involves downloading the updates to a third computer, verifying their contents and checksums, then burning them onto a CD for installation to the GEMS server.

2. Disable any unnecessary services with the assistance of qualified IT personnel as described in the Diebold Client Security document (Diebold Election Systems, January 11, 2007), section 4.5.

3. Install and regularly update a malware detection program such as McAfee anti-virus software.

4. Evaluate the use a drive encryption program such as TrueCrypt or BitLocker (Windows Vista only) on the GEMS servers. This type of software encrypts/decrypts data stored on the hard disk in real-time. If an attacker removes the hard disk and attempts to mount it on a different machine, the data will be unreadable without the encryption keys.

5. Regularly inspect both Windows event logs and database logs for suspicious activity. The frequency of inspection should be on a fixed schedule and at a minimum include an inspection before, during, and after an election.

Appendix F: Ballot and Election Equipment Distribution and Chain of Possession

1 Ballot and Election Equipment Distribution and Chain of Possession

The process of holding a statewide election begins long before Election Day. The following section is a general description of the locations and movements of election ballots and voting machines through one election. Because Alaska communities are so diverse in their size and accessibility, there are exceptions to the processes not represented here. The state uses standard procedures to keep the process as consistent as possible, as we illustrate in several diagrams. Section 1.1 shows the icons used in those diagrams. We describe the creation and distribution of ballots both for hand counting precincts and for use in the optical scan voting machine (Sec 1.2); the general dispersion and return of the optical scan voting machines (Sec. 1.3) and touch screen voting machines (Sec. 1.4) from storage to the respective precincts and back to storage. The movements of the machines include the merging of memory cards with the voting machines and their removal and return to Juneau after the election.

With the large number of polling locations throughout Alaska, the distribution and storage requirements have always been a logistical challenge. For the majority of the life of any voting machine and memory cards, they reside in secure storage. From the beginning of an election cycle, there is the need to remove the machines from storage, test as appropriate, prepare, and distribute.

When ballots and voting machines are stored and when they are in transit there are challenges in protecting them from damage and the potential for unauthorized access. Accessibility, accountability, training, and documentation with regard to the chain of custody should be monitored and reviewed.

Icons Used in the Voting Process Diagrams

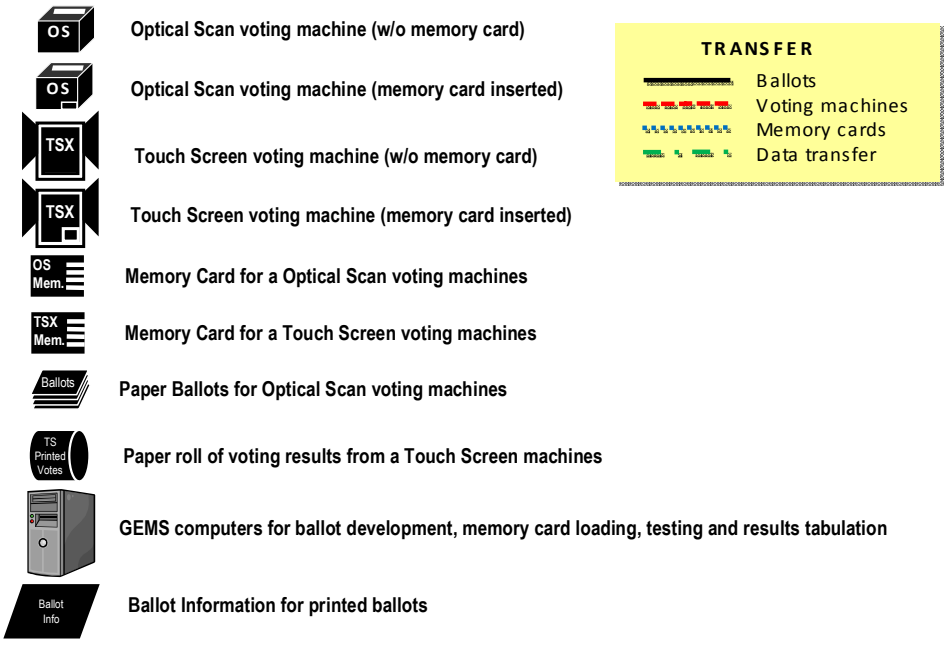


Figure 1 - Voting Process Diagram Icons

Optical Scan Ballots and Hand-Count Ballots

The following diagram and legend describe the movement between locations and over time for the optical scan ballots and the hand counted ballots between ballot design in Juneau (based on the candidates' applications filed with the Division of Elections) and other ballot issues. The regional election offices provide precinct-by-precinct official counts of registered voters and quantities of ballots needed for each voting location.

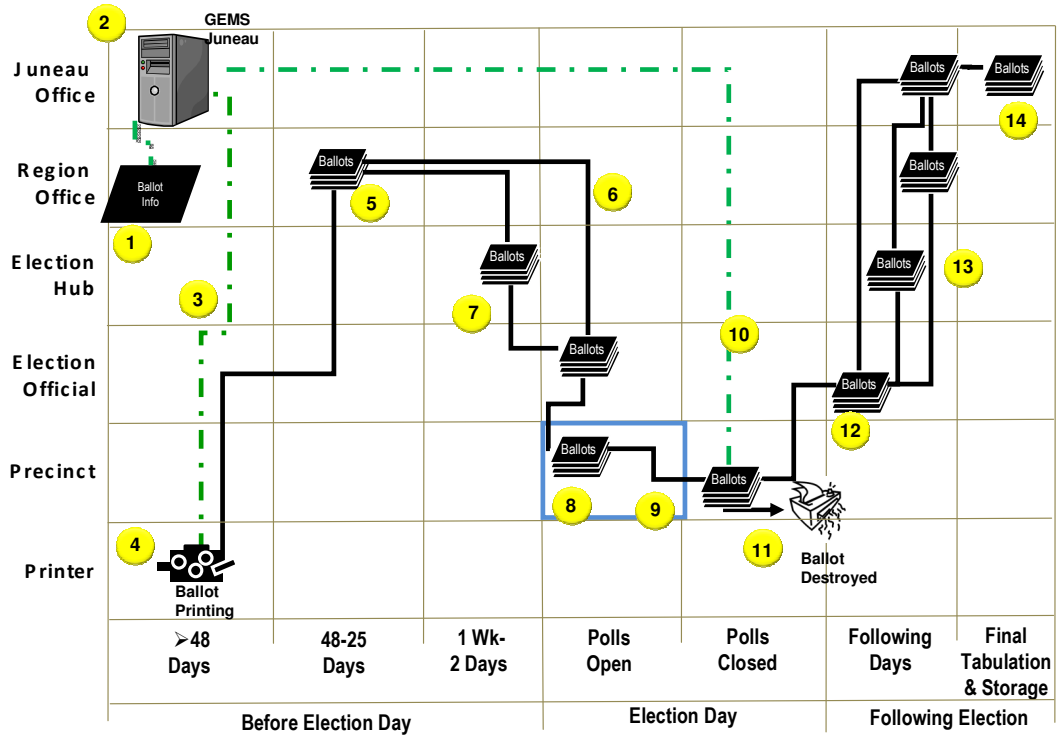


Figure 2 - Optical Scan Ballots and Hand-count Ballots – Chain of Possession

1. Regional offices submit the quantity of ballots needed for each voting location to the Director of Elections office in Juneau.
2. GEMS programmed with candidate information and layout.
3. Ballot information and precinct quantities are sent electronically to the ballot printer.
4. Ballots are sequentially numbered, printed and shrink-wrapped in quantities of 25.
5. Ballots are shipped by the printer to the Division of Elections offices in Anchorage, Fairbanks, Juneau, Mat Su and Nome.
6. Ballots for locations in rural Alaska are mailed by delivery confirmation to local election officials
7. Some locations ballots are shipped to hubs prior to distribution to election officials, while those locations within driving distance to a regional office picks up the ballots directly from the election supervisor.
8. Ballots are brought to polling places the morning of the election by an election official
9. After polls have closed all ballots are secured.

10. The OS voting machine transmits the results to Juneau. If hand counted, the results by the Regional offices to are called into Juneau. The unused ballots are destroyed.

11. The ballots are secured by the local election officials.

12. All ballots, along with signatures, memory cards and ballot statement are combined, sealed and returned to the Division of Elections. The route back is same as respective route ballots took to the polling places from a Regional Office.

13. All voted ballots are retained in Juneau for recounts and final archiving.

1.2.1 Optical Scan Machines (OS) and Memory Cards

Optical Scan machines are stored at Regional Election Offices or at selected hubs between elections. The memory cards for the Optical Scan machines are stored in Juneau between elections. After an election, OS machines are returned to their respective storage locations and the memory cards are all returned to Juneau for any necessary review and to be stored. Optical Scan machines, when in use, are locked in place on top of a black poly-carbon ballot box. These boxes are distributed separately and can be positioned at polling places before the morning of the election. They are designed to hold the scanned ballots and contain a side slot and separate chamber to hold any ballots voted but not scanned.

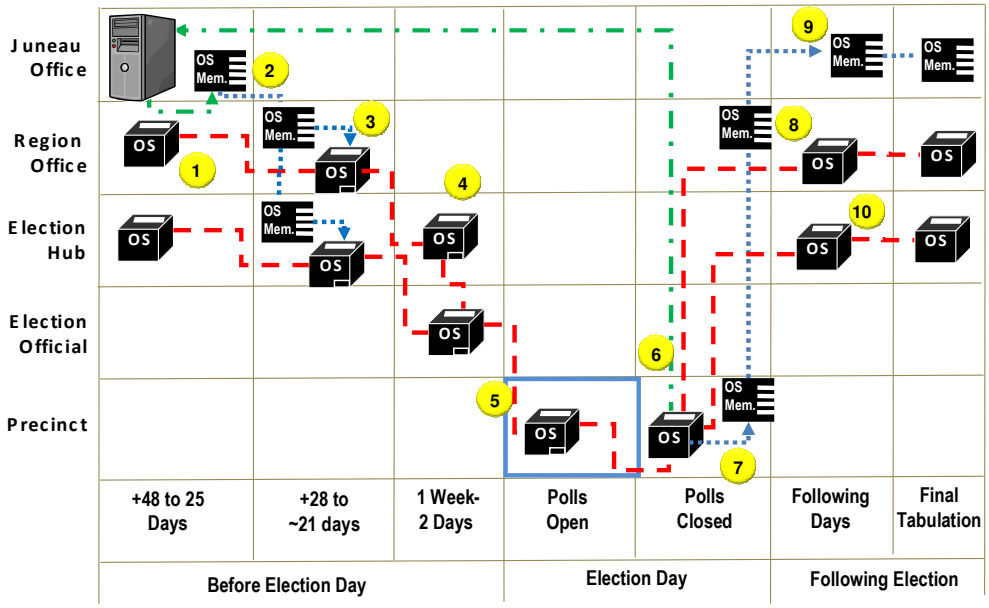


Figure 3 - Optical Scan Machine (OS) & Memory Card – Chain of Possession

1. Optical Scan Voting Machines (OS) are stored and tested at the Regional Offices or stored and tested at selected hub locations.
2. GEMS programs the memory card in Juneau. They are tested by the State Review Board there before being sent to the Regional Offices.
3. The memory cards and the OS machines are tested at the regional offices by the Regional Accu-Vote Board or in hub communities by Accu-vote coordinators.. The memory cards are inserted into the machines and sealed.
4. The OS voting machines are distributed to the precinct officials for placement on Election Day either from the Regional office or a hub.
5. The voting machines are placed at the precinct the morning of the election and are tested before the polls are open.
6. After the polls are closed, the ballot results are printed and signed-off by the election board and then are sent by the OS machine to GEMS in Juneau.
7. The memory card is removed and ballots, memory card, printed results and ballot statement are sent to Juneau either directly or through the Regional Office.
8. The memory cards are returned to Regional Offices when the cards can be delivered directly. Off the road system, cards are sent to Juneau directly.
9. The OS memory cards and printed results are received by the Juneau office for any needed review and final storage. At the Director's office, in Juneau the cards and printed results are used to resolve unexplained discrepancies.
10. The OS machines are returned to their originating Regional Office or hub for storage.

1.2.2 Touch Screen (TSX) Voting Machines and Memory

Touch Screen (TSX) voting machines must be available at each voting location to assist disabled voters who need special assistance. Electronically these are more sophisticated machines and are programmed with the ballot information both as a visual ballot and as an audible ballot for the blind. The TSX machine can be used by any voter, but are intended for use by disabled voters. As seen in the following flow diagram, as each voter votes, the machine produces a printed version of the voter’s choices, which the voter can see and confirm before casting a ballot. Once the ballot is cast on the TSX, the printed ballot is wound into a storage canister in the machine, which is removed after the polls close and returned along with the results stored in the memory card. The machines are returned to the locations where they are kept between elections. Because of the size and weight (60 lbs.) of the TSX machines, some are stored at communities between the primary election and the subsequent general election.

The printed records from TSX machines are treated as “official” ballots for their return to regional offices and to Juneau. Likewise, the TSX memory cards are treated like the memory cards from the OS machines.

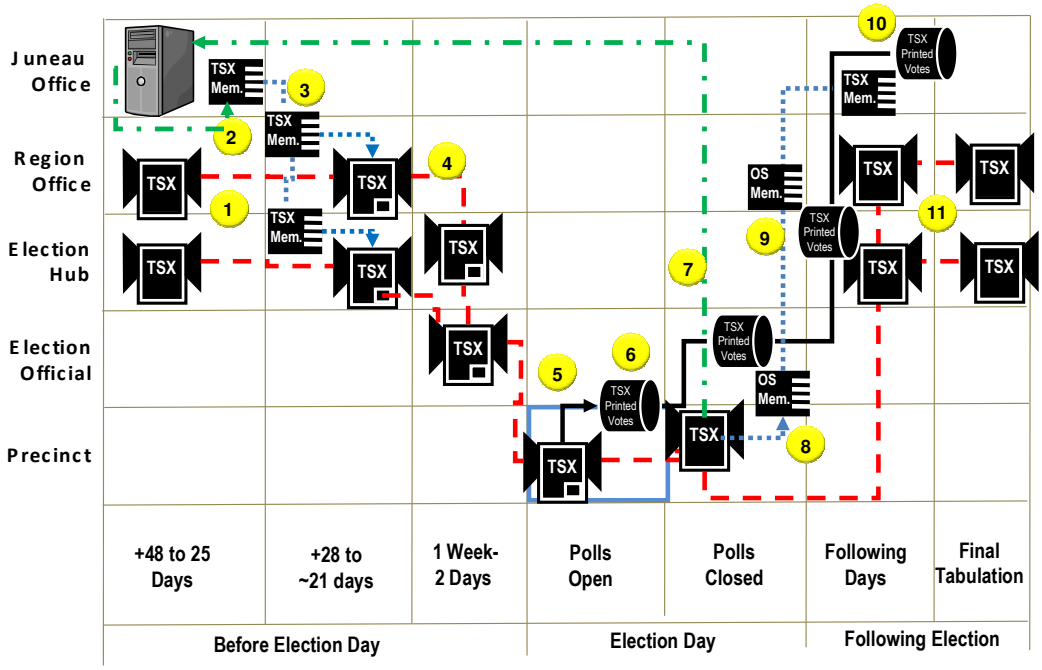


Figure 4 - Touch Screen (TSX) Voting Machine & Memory Card – Chain of Possession

1. Touch Screen Voting Machines (TSX) are stored and tested at the Regional Offices and at selected hub locations.

2. GEMS programs the TSX memory card in Juneau. They are tested there by the State Review Board before being sent to the regional offices.

3. The memory cards and the TSX machines are tested at the regional offices by the Regional Accu-Vote Board. For those machines stored in hub locations, the memory card is sent to the hub location. The memory cards are inserted, either at the regional office or hub location, into the machines and sealed before being distributed.

4. The TSX voting machines are distributed to the to precinct election officials for placement on Election Day.

5. One TSX voting machine is positioned at each of the polling places for use while the polls are open.

6. As voters use TSX voting machines, their choices are printed onto an enclosed printed roll. The voter can review and confirm their choices on the printed version of the ballot. Upon approval, the results are reeled into a container within the machine and stored. The individuals' results are also stored on the memory card in the AV-TSX machine.

7. After the polls are closed, the final results are both printed from the AV-TSX machine and the results are transmitted electronically to GEMS in Juneau with t he exception of results in hand-counted precincts and those that are called in to Regional offices and up-loaded to Juneau.

8. The memory card, printed ballots, printed results summary are removed after the polls are closed and the AV-TSX machine's results are transmitted.

9. The AV-TSX memory cards are returned to the Regional offices or hub for delivery to Juneau or in some cases sent directly to Juneau..

10. The memory cards and the printed AV-TSX ballots rolls are returned to Juneau for review and, in the case of the ballot rolls, archiving.

11. The AV-TSX machines are returned to the Regional Office or hub where they originated for storage.

The information regarding movements is general. Actual movements between the beginning and end of an election cycle can be quite complex.

Premier Election Solutions

California Tamper Evident Security Seal Document

Version 2
January 17, 2008

Premier Election Solution
Tamper Evident Security Seal Document

The following document illustrates the recommended placement of tamper evident security seals on Premier Election Solution (Premier) equipment. The applicable equipment includes the AccuVote-OS (optical scan) and the AccuVote-TSX (touch screen). Premier is using best practices on the placement of security seals based on discussions and interviews with several California counties. The placements of those seals are recommendations to mitigate any potential tampering of the AccuVote-OS and AccuVote-TSX units.

Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional placement of seals on the voting equipment, depending on the county's security seal policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-OS and AccuVote-TSX units.

Premier is illustrating where the placement of the security seals could be placed on those units. As far as the actual security seals, Premier does not recommend a specific vendor. However, tamper evident security seals from vendors such as Intab and Seton have been used on the equipment with success. There are illustrations of those seals within this document.

All seals used on Premier equipment should be serialized and tamper evident. Additionally, the security seals must be logged and tracked by the authorized election officials and verified by the poll workers prior to using the voting equipment. This verification process ensures the equipment has been thoroughly checked and verified against any potential tampering of those units

In some seal application areas, a choice of different seal types is available. In other instances, the choice to apply multiple seals is possible. The following outline pictures will demonstrate the use and location of wire anti-tamper evident labels, wire seals, plastic (rat tail) seals, and spring lock seals on the AccuVote-OS and AccuVote-TSX.

The following is a list of the seal application areas by the equipment type. The equipment type also includes the AccuView Printer Module (AVPM) which contains a security canister used for housing the voter-verifiable paper audit trail. The AVPM security canister is secured using a spring lock security seal or a tamper evident security seal.

Seal Application Areas by Equipment Type

- AVOS
  - Memory Card seal
    - Wire Security Seal

- AVTSX
  - Memory Card Slot seal
    - Anti-Tamper Evident Security Seal Label

- AVTSX Front Panel Door seal
  - Wire Security Seal
  - Plastic (rat tail) Security Seal

- AVPM
  - Printed Receipt Security Canister Seal
    - Spring Lock Security Seal
    - Anti-Tamper Evident Security Seal Label

There are several types of tamper-evident seals and labels used on the AccuVote-OS and AccuVote-TSX units. The following seals have been used on the AccuVote-OS and AccuVote-TSX security seals. The wired and spring lock seals have been used for the memory card slot on the AccuVote-OS unit. The tamper evident security seals and spring lock seals have been utilized on the AccuVote-TSX units.

Wire Security Seal (Passive RFID Tool less Roto Tag)

Spring Lock Plastic Security Seals (Heat Stamped and Consecutive Numbering)

Tamper Evident Security Seals Label (1 by 3 inches, serialized)

Tamper Evident Security Seal Label (1 by 3 inches, bar-coded and sequential numbered)

Tamper Evident Security Seal (10 inch pull tight seal, Heat stamped and serialized)

AccuVote-OS Security Seal Locations

The following are recommended locations for the placement of security seals on the AccuVote-OS unit. Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional seal placements, depending on the county's security seal policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-OS. At a minimum, a jurisdiction should seal the following locations on the AccuVote-OS unit when used in the precincts:

- Memory Card Slot
- Sealed over the front of the AccuVote-OS unit over the "seam" on the AccuVote-OS unit, and / or in the rear of the AccuVote-OS unit over a screw hole as well as over the "seam" on the back of the AccuVote-OS unit

All of the security seals must be logged, serialized and verified by the poll worker prior to using the equipment on Election Day. The jurisdictions could deploy a seal verification log which the poll worker could verify the security seal with the seal verification log document.

See the photos below for an illustration of the security seals on the AccuVote-OS.

AccuVote-OS Memory Card Slot Sealed with a Security Seal

AccuVote-TSX Security Seal Locations

The following are recommended locations for the placement of security seals on the AccuVote-TSX unit. Counties are recommended to use this placement of seals, along with augmenting the security seal placements with additional seal placements, depending on the county's security seal placement policies and procedures. The recommended placement of seals on the unit should not preclude a county from continuing to utilize their best practices regarding seal placements on the AccuVote-TSX. At a minimum, a jurisdiction should seal the following locations:

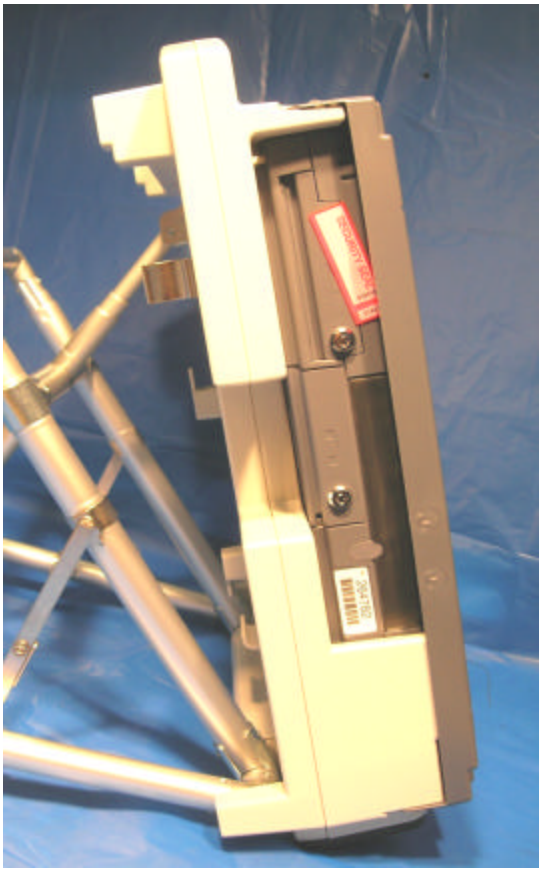
- AVTSX Memory Card Slot and /or On/Off Slot
- On the AccuVote-TSX over a screw hole, which would also cover the "seam" on the AVTSX unit

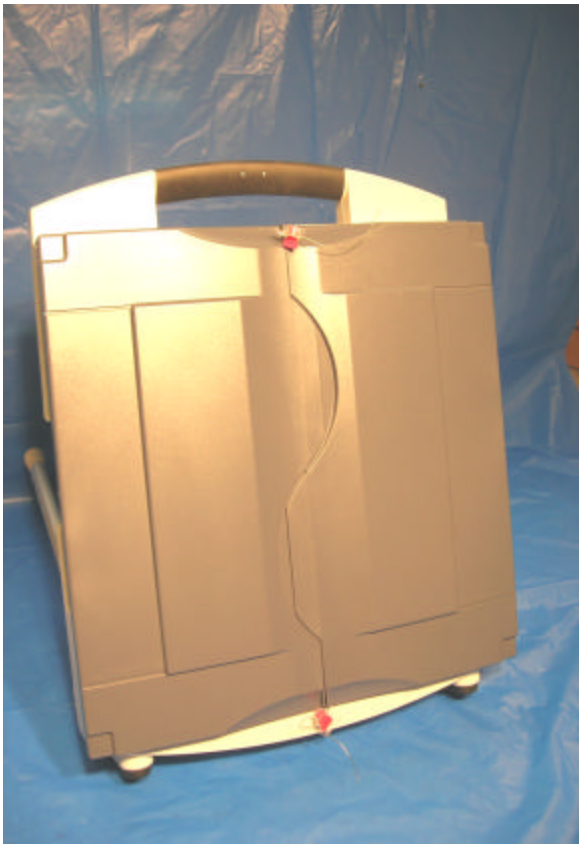
Additionally, a security seal should be placed sealing the AccuVote-TSX "doors".

All of the security seals must be logged, serialized and verified by the poll worker prior to using the equipment on Election Day. The jurisdictions could deploy a seal verification log which the poll worker could verify the security seal with the seal verification log document.

See the photos below for an illustration of the security seals on the AccuVote-TSX.

Illustration of AccuVote-TSX Security Seal Placements



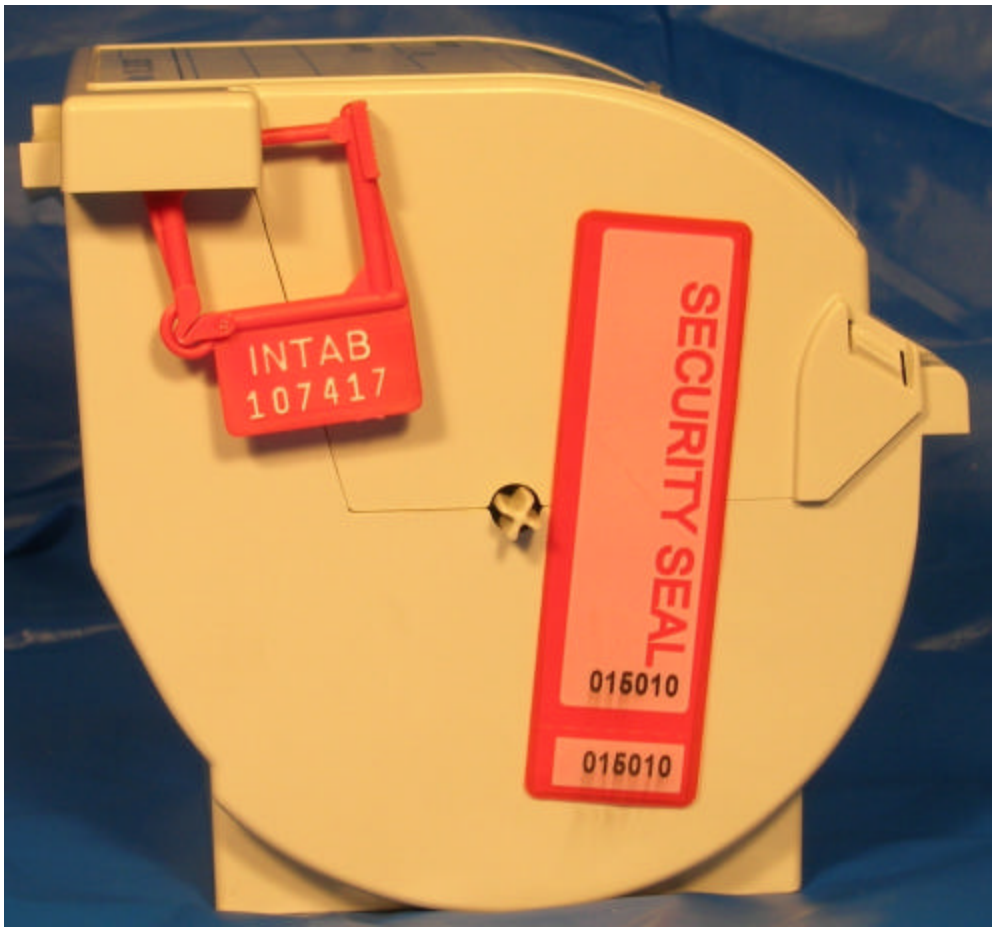


AccuView Printer Module (AVPM) Security Seal Locations

The following are recommended locations for the placement of security seals on the AVPM. At a minimum, a jurisdiction should seal the following locations:

- On the AVPM security canister with a tamper evident security seal sealed over the opening of the AVPM security canister; or
- With a springlock seal on the security canister

The security seal needs to be placed on the security canister when the security canister has been fed with paper, and the security canister has been closed. See the photos below for an illustration of the security seals on the AVPM.



Appendix H – Security Training

General instructions to poll workers

To ensure 5 votes on AV-TSX poll workers vote at the end of the day. Poll workers should vote at the end of the day. If there are more than 1 but fewer than 5 votes cast on AV-TSX, then they should cast their votes on AV-TSX machines.

Tampering doesn't need to be sophisticated. Attempts at election fraud can look more like vandalism that high tech computer hacking. If someone is worried about losing an election in specific precinct, that person might try to prevent people from voting for opponent by causing a disruption.

Election results would also be destroyed if someone spilled liquid on to the AV-TSX printer. The printer paper absorbs liquids, so a spill could leak though plastic cover and absorb into the paper on the spool.

Don't allow loitering in the area around voting booths.

Don't allow people to bring food or beverages into voting booths.

Equipment used in absentee voting locations is exposed to tampering for several days. People in charge of elections in absentee locations need to exercise vigilance and ensure that voting equipment is locked in secure storage areas when a voting official is not present.

Tamper evident seal inspection on AV-TSX and AV-OS machines

Regional Offices

Prior to election

1. Prior to opening polls. Keep list of all machines/precincts where poll workers have reported that tamper-evident seals have been broken.
2. After election. Test and inspect memory cards from machines where seals have been broken. Votes cast on these machines may be subject to 100% manual tally.

Precincts

Prior to opening polls

1. Prior to opening polls. Inspect tamper evident seal on the AV-TSX machine. DO NOT REMOVE SEAL.
2. If seal is not broken, check "no" on checklist.
3. If the seal is broken, check "yes" on the checklist and notify Regional Director.

Appendix I – AV-OS Shipping Container Example

1 Description

The AccuVote optical scan (AV-OS) machines currently use cardboard boxes with hard cell foam inserts. These cardboard boxes are prone to deterioration over time, especially when considering the frequency use they receive. An assessment of the reliability of the AV-OS machines found a measurable number of AV-OS repairs required resulting from physical damage incurred during shipment or transport.

An improved shipping container would reduce the number of failures due to physical damage during shipment and transport. Initial procurement of new shipping containers requires the purchase of a new case for each AV-OS machine. The cases purchased for use in the shipment of AV-OS machines would make suitable, robust storage containers as well, further protecting the devices from damage. The selected shipment and storage container should allow the Division of Elections to lock the case with a tamper seal.

2 Example Case and Cost Estimate

The dimensions of the AV-OS machine are 16 inches X 14 inches X 3 inches. These dimensions can be accommodated by a Pelican™ Products 1600 series case. The 1600 series case has interior dimensions of 21.43 inches X 16.50 inches X 7.87 inches. Pelican™ 1600 cases are watertight, crushproof and dust proof making them ideal for transport and storage of sensitive electronic equipment. Custom configurable foam interior lining allows the case to be fitted to the AV-OS machine. Pelican™ cases also include openings for case security (lock or tamper seal insertion).

It is recommended that the Pelican™ 1600 case or a similar product is purchased for the storage and transport of all AV-OS machines owned by the Division of Elections.

The Pelican™ 1600 case is available at an average street price of $160. The Division of Elections has a total of 290 AV-OS machines in its possession. This results in a total cost of approximately $46,400.00 to procure new cases. In addition to the procurement cost there is labor associated with configuring each case for the AV-OS machines. An estimate of 30 minutes per case to configure the foam lining results in a labor estimate of 145 man hours.

A manufacturer cut sheet taken from the Pelican™ Products website is included on the following page.

Print | Close Window

Uncontrolled document as of April 28, 2008. Refer to website for up to date specifications.

CASES 1600 Case

1600 Case

- Watertight, crushproof, and dust proof
- Open cell core with solid wall design - strong, light weight
- Automatic Pressure Equalization Valve
- O-ring seal
- Comfortable rubber over-molded handle
- Stainless steel hardware and padlock protectors
- 2 level Pick 'N' Pluck™ with convoluted lid foam
- Personalized nameplate service available
- Unconditional Lifetime Guarantee of Excellence

1600 Case Configurations

Cat. #	Description
1600	1600 Case
1600NF	1600 Case (No foam)
1604	1600 Case with Padded Dividers

 Black
 Silver
 Orange
 Yellow
 OD Green*
 Desert Tan

*OD Green available upon request

1600 Case Specifications

Exterior Dimensions (L x W x D)
24.25" x 19.43" x 8.68" (61.6 x 49.3 x 22 cm)

Interior Dimensions (L x W x D)
21.43" x 16.50" x 7.87" (54.4 x 41.9 x 20 cm)

Lid Depth
1.75" (4.4 cm)

Bottom Depth
6.12" (15.5 cm)

Total Depth
7.87" (20 cm)

Weight with Foam
14.11 lbs. (6.4 kg)

Weight without Foam
13 lbs. (5.9 kg)

Buoyancy Max.
74.96 lbs.
(34 kg)

Range Temperature
-10 / 210° F
(-23 / 99° C)

Personalized Nameplate Available

1600 Case Certificates

• IP67 (1 meter submersion for 30 minutes)
• MIL C-4150J • Def Stan 81-41/STANAG 4280 • ATA 300

1600 Case Accessories

Cat. #	Description	Sug. Retail
1600IP	Instapak Quick® RT	US$47.95
1601	4 pc. Replacement Foam Set	US$99.95
1602	Pick 'N' Pluck™ Sections Only (set of 2)	US$81.95
1603	Replacement O-ring	US$5.25
1605	Padded Divider Set Only	US$158.95
1609	Lid Organizer	US$45.95

Appendix J - AccuVote Communications System Description

1. Introduction

The purpose of this document is to analyze and document the configuration and topology of the State of Alaska Division of Elections AccuVote communications network. The goal of this analysis is to identify any potential vulnerabilities and to recommend enhancements to the Division of Elections.

2. Network Topology

The Division of Elections (DoE) AccuVote communications network is utilized to transmit preliminary, unofficial election results to the DoE director's office host GEMS upon the close of polls at each precinct. These results are tabulated by the director's office GEMS and are provided as preliminary, unofficial results to the public.

The Division of Elections AccuVote communications network is comprised of the following network transmission types.

1. AccuVote Optical Scan (AV-OS) and AccuVote Touchscreen (AV-TSX) Precinct Reporting

Each voting precinct utilizing AV-OS and AV-TSX machines reports preliminary results using an internal modem which is fully tested prior to each election. The internal modem is connected to a local Public Switched Telephone Network (PSTN) jack at the precinct. Using the public telephone network a communications channel is established between the DoE director's office GEMS server and the local precinct equipment. A total of 48 analog modems in the director's office are configured to handle the incoming requests as precincts are closed across the State of Alaska.

The AV-OS and AV-TSX machines are configured to utilize the Secure Socket Layer (SSL) protocol to ensure that the communications channel is secure. Use of this protocol minimizes eavesdropping vulnerabilities over the communications channel.

2. GEMS Handcount Reporting

The regional office GEMS servers are used following an election to enter handcount ballots into the AccuVote system. The handcount ballots are collected and a data entry technician enters the ballots into the region's GEMS software. When all of the ballots have been captured in the GEMS server the ballots results are transmitted to the GEMS in the DoE director's office in Juneau using an analog modem.

Ballot results transmitted in this manner are connected to PSTN in the same manner as the precinct AV-OS and AV-TSX machines. In the case of Region 3 the PBX is interconnected using a dedicated T-1 circuit provided by the telecommunications carrier General Communication Inc. An option 81 Nortel PBX located in the Juneau, Alaska director's office terminates all transmissions into the DoE director's office.

A total of 6 regional GEMS servers are used in each election to enter handcount ballots. The GEMS servers are allocated based on the number of handcount precincts present in a region. A regional breakdown of the number of handcount precinct as well as the number of regional GEMS servers is provided below.

Region	Handcount Precincts	GEMS Servers
Southeast – Region 1	18	1
Anchorage and Matsu – Region 2	1	1
Fairbanks and Interior – Region 3	45	2
Nome, Barrow, West Coast – Region 4	85	2

Each regional GEMS server is configured to utilize the Secure Socket Layer protocol when transmitting data between itself and the DoE director's office GEMS.

3. Recommendations

The current Division of Elections communications network appears to be implemented in a reasonable, robust manner. Built-in safeguards such as implementation of the SSL protocol are in use as suggested by Premier Election Solutions.

The State of Alaska Election Security Project was made aware that the State of Alaska will be transitioning its current analog phone system to a full voice over IP (VoIP) system in the future. It is recommended that a subsequent analysis of this network be performed once the details of the new voice network are finalized. Implementation of a VoIP network presents a different set of security risks to data transmission and these risks and vulnerabilities should be assessed before the network is used for a subsequent election.

Daisy Chain Serial Server Connection

Active GEMS Server

SSL

SCSI

Digiport 16EM Serial Server

Digiport 16EM Serial Server

Digiport 16EM Serial Server

Multitech Rack Mount Modem 16 Each T5600BR-V92

Multitech Rack Mount Modem 16 Each T5600BR-V92

Multitech Rack Mount Modem 16 Each T5600BR-V92

16 Port NT8D09

16 Port NT8D09

16 Port NT8D09

Backup GEMS Server

Juneau Director's Office

Nortel Option 81 Private Telephone Exchange (PBX)

Private Line Circuit

Analog Modem

SSL

GEMS Server

handcount ballots (18 Precincts)

SSL modem **AV-OS (71 Precincts)**

SSL modem **AV-TSX (89 Precincts)**

Voting Precincts

Region 1 Southeast

Analog Modem

SSL

GEMS Server

handcount ballots (1 Precinct)

SSL modem **AV-OS (151 Precincts)**

SSL modem **AV-TSX (152 Precincts)**

Voting Precincts

Region 2 Anchorage and Matanuska Valley

handcount ballots (85 Precincts)

SSL

GEMS Server

Analog Modem

SSL

GEMS Server

Analog Modem

SSL modem **AV-OS (12 Precincts)**

SSL modem **AV-TSX (97 Precincts)**

Voting Precincts

Region 4 Nome, Barrow and West Coast

Public Switched Telephone Network

Private Telephone Exchange (PBX)

Analog Modem

SSL

GEMS Server

Analog Modem

handcount ballots (45 Precinct)

SSL

GEMS Server

SSL modem **AV-OS (56 Precincts)**

SSL modem **AV-TSX (101 Precincts)**

Voting Precincts

Region 3 Fairbanks and Interior

State of Alaska Election Security Project

DoE AccuVote Network Topology			
Name:	AccuVote Election System Network Interconnection Topology		
Drawn By:	Mark Ayers	Date:	*4/13/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*1 of 1*

Appendix L - AccuVote Reliability Assessment

1. Introduction

This document assesses the reliability of the AccuVote system components operated by the State of Alaska Division of Elections. The Division of Elections maintains records of AccuVote Optical Scan equipment that is returned to Premier Elections Systems for repair with varying detail by region. These records provide information regarding the failure mode and the repairs required to return the machine to "as new" condition. Records regarding the AccuVote Touch Screen and GEMS systems are not maintained in sufficient detail to evaluate reliability trends.

This document describes the reliability requirements as stated in the Voting System Standards (VSS) 2002 (2002) specification and describes the concept of reliability as it relates to the Division of Elections' system. A brief discussion of the VVSG Recommendations to the EAC (2007) is provided as this document provides a significant improvement in the specification of reliability performance regarding electronic voting systems over the 2002 VSS. An evaluation of the limited data set provided by the Division of Elections offers some insight regarding the failure trends and observations. Recommendations are made regarding ways to improve the reliability and performance of the AccuVote Optical Scan hardware.

2. Reliability Performance Specifications

The reliability performance required from the AccuVote hardware and software is defined in the Federal Election Commission's 2002 Voting Systems Standards. Conformance with these specifications is required by state aw. Conformance with these specifications is established through the Independent Testing Authority (ITA) certification process. The 2002 VSS uses the term "system" in several instances when discussing both reliability and availability.

Taken in the context of the 2002 VSS, the term "system" can be taken to imply a single voting machine under test. This is consistent with the ITA test report results. It is our opinion that this interpretation is inconsistent with commonly accepted reliability theory and that the values specified by the 2002 VSS result in reliability certifications which are of little value to the Division of Elections. Reliability and availability are statistical quantities and must be taken in the context of a statistically significant volume of machines or units. In the case of the State of Alaska this would mean considering a system which is sized at least as large as one of Alaska's four regions. Further discussions in this section which use the term "system" will clarify whether the intent is to indicate a single voting machine (hardware and software) or a set of voting machines.

The minimum reliability and availability required for certification in the State of Alaska are specified in the 2002 VSS.

Reliability is defined in the 2002 VSS in terms of the statistical parameter mean time between failures (MTBF). This parameter defines the average interval between which failures occur. A failure is defined as any event where the system (an individual machine or set of machines) fails to perform one or more functions or exhibits behavior where performance is degraded to an unusable condition for a period of greater than 10 seconds. The MTBF is defined in the 2002 VSS as having a minimum value of 163 hours.

System availability is the probability that the system performs the desired functions at any instant in time under stated conditions. The VSS 2002 standard provides guidelines for both the

calculation and evaluation of the system availability. Specific system components are required to meet availability specifications within the VSS 2002 guidelines. In the case of the AccuVote optical scan (AV-OS) machines the functions of voter selection recording and paper ballot encoding must meet the availability requirement. The AccuVote touch screen (AV-TSX) availability requirement applies to the recording and storage of voter ballot selections. In both the AV-OS and AV-TSX cases the consolidation of the vote data requires that the Global Election Management System (GEMS) also meet the availability requirement. The VSS 2002 standard specifies a minimum system availability of 99%.

Upon reviewing the ITA certifications documents the evaluation of reliability and availability are subject to interpretation and do not seem to provide useful performance measures. Review of the Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission (2007) specification provides a significant change in the performance specifications associated with voting system reliability. This specification has not yet been ratified and is not in force for the State of Alaska. A review of its contents is valuable for the assessment of future voting system performance specifications and evaluation of those changes against the system currently in operation.

3. Division of Elections System Performance

Evaluation of the Division of Elections system using empirical data is problematic. Comprehensive records regarding failures of the AV-OS, AV-TSX and GEMS system components do not exist. As such the statistical data here is based on records kept by Region III (Fairbanks) and Region IV (Nome, Barrow, West Coast of Alaska). Qualitative information can be gleaned from these records regarding AV-OS and AV-TSX performance weaknesses and areas in which improvements might be made.

3.1 System Description

The State of Alaska Division of Elections operates a Premier Election Solutions AccuVote system with the following AccuVote component counts. The counts presented in Table 1 refer to precinct counts. The Division of Elections maintains additional AV-OS and AV-TSX machines as spare units in the case of a failure.

Region	AV-OS	AV-TSX	GEMS
I - Southeast Alaska	71	89	1
II - Anchorage / Mat-su	151	152	1
III - Fairbanks / Interior	56	101	2
IV - Nome / Barrow / West Coast	12	97	2
Juneau Director's Office	0	0	2
Total	*290*	*439*	*8*

Table 1. AccuVote System Component Count by Region

The GEMS servers in the Juneau Director's office operate in a redundant configuration where a backup server available in the case that a failure of the primary server occurs. This backup server is configured prior to each election to exactly mirror the configuration of the primary GEMS server. In the case that the primary GEMS server fails the backup server would quickly be brought into service. A minimal service outage would result in the case of a primary GEMS server failure. Redundancy for the backup server is not provided.

Precinct level machines are operated in a non-redundant configuration. Two different deployments of AV-OS and AV-TSX machine are used depending on the population of each community. In larger communities a single AV-OS and AV-TSX is allocated to each voting precinct. Smaller communities utilize hand-counted paper ballots or optional use of the AV-TSX machines.

A non-repairable failure of the AV-TSX voting machine results in voters being directed to use the AV-OS machine in that precinct (where available). Failure of the AV-OS machine results in a precinct hand count. The paper ballot reliance built into the Division of Elections system results in a system in which no failure can occur which would cause a voter to be turned away during an election.

During live elections the Division of Elections employs “rovers”. Rovers are trained on-call helpers responsible for assisting with trouble calls during an election. They are trained to replace malfunctioning equipment and to assist election workers in ensuring that the election hardware works properly on election day. Rovers serve to increase the availability of AV-OS and AV-TSX machines by reducing the equipment outage duration associated with a failed component in urban areas. Rovers are employed by the Division of Elections in Anchorage, Fairbanks, Juneau, Kenai Borough, Sitka, Kodiak, Valdez, Nome and the Matanuska Valley. In all other communities the failure of an AV-OS or AV-TSX results in it being removed from service and the ballots hand counted.

Although a rigorous academic reliability analysis of the Division of Elections AccuVote system does not exist for public review the historical performance of the system is very good. The Division of Elections reliance on paper ballots as the final ballot of record ensures that in no circumstance will a voter be turned away because of equipment malfunctions. Failures of system components result in an increase in election worker resource requirements but do not affect the outcome of an election.

3.2 Premier Election Solutions Reliability Models

The VSS 2002 standards set specific requirements regarding the reliability and availability of election systems (as defined in the 2002 VSS). Certification of the AccuVote system used by the Division of Elections against the VSS 2002 standard ensures compliance with the reliability requirements. Section 3.4.5 of the VSS 2002 requires vendors to specify the configuration of systems to the ITA for evaluation. This configuration specification includes sparing recommendations, maintenance / repair staffing recommendation and system configurations required to ensure that the required availability is met.

Unfortunately, the content of these technical details remains closed to public disclosure and these documents were not reviewed as part of this analysis.

3.3 Division of Elections Failure Data

The State of Alaska Division of Elections has maintained repair and maintenance records for the AV-OS machines in Region III (Fairbanks and Interior) and Region IV (Nome, Barrow and West Coast of Alaska) of the voting system. These records were reviewed and the primary failure modes were determined.

Repair records for Region III and Region IV are not in the same format and as such the resultant analysis is qualitative in nature.

Region III maintenance and repair data provided to the SOAESP team records repair activities for the AV-OS machines dating back to 1998. A total of 37 failures are recorded in the Region III AV-OS repair records between 1998 and 2006. It was recorded that four (4) of the failures were coincident with physical damage to the machine. In many cases the machines housing was cracked or damaged and had to be replaced.

Failure Mode	Number of Failures
Ballot Reader	21
Modem	7
Liquid Crystal Display	4
Power Supply	2
No Trouble Found by Premier	5
Printer	0

Table 2. Region III AV-OS Failure Modes

Review of this data shows that the AV-OS ballot reader is the primary component failure mode. The percentage of failure column in Table 2 does not sum to 100% because in several instances a multiple failure was discovered during the repair of the AV-OS machine. During the period between 1998 to 2006 a total of 28 unique machines failed in a manner requiring repair by Premier Election Solutions. Table 1 indicates that in Region III 56 AV-OS machines are in use which results in the unique failure of exactly 50% of AV-OS machines in the 1998 to 2006 time period.

Region IV maintenance and repair data provided records of the maintenance activity for both the AV-OS and AV-TSX machines over the time period from 2000 to 2007. Failure data for the 17 AV-OS machines in Region IV are provided in Table 3.

.

Failure Mode	Number of Failures
Ballot Reader	7
Modem	1
Liquid Crystal Display	0
Power Supply	2
Printer	1

Table 3. Region IV AV-TSX Failure Modes

Failure data from Region IV confirms that results seen in the Region III data indicating that the ballot reader is the least reliable component in the AV-OS machine.

Failure data for the 102 Region IV AV-TSX machines is provided in Table 4.

Failure Mode	Number of Failures
Printer	7
Modem	4
Screen	2
Enclosure	4
Memory Card Slot	1

Table 4. Region IV AV-OS Failure Modes

The data in Table 4 shows that printer failure is the primary mode of failure for the AV-TSX machines.

4 Recommendations

Review of the Division of Elections empirical data log with the 2002 VSS and 2007 VVSG indicate a high operational reliability and availability for the AccuVote system in the State of Alaska. The specifications provided by the 2002 VSS certification provide little insight or value regarding an AccuVote system consisting of hundreds of machines which operate simultaneously during an election. In spite of an apparent lack of publicly available academic rigor regarding reliability and availability of the system operated by the Division of Elections the practical reliability and availability are extremely high.

The reliance on the paper ballot as the final ballot of record provides an inherent improvement in system reliability which could never be achieved in a system which exclusively uses Direct Recording Electronic (DRE) voting terminals. Failure of electronic components in the current Division of Elections increases the resource dependence by initiating the hand count process but no time jeopardizes a precinct's ability to serve voters.

Although the current system is very robust and effective, we are making recommendations which should prove to incrementally reduce machine maintenance and improve reliability. More robust functional and logic and accuracy testing as detailed in Appendices M and N are recommended. Increased functional testing scope would serve to better detect hardware failures prior to equipment shipment and will reduce day of election field failures.

Better storage and transport containers for AV-OS are also recommended. Empirical maintenance data review indicates a measurable number of AV-OS machines experiencing physical damage during shipment and transport. The correlation between the transportation of the AV-OS machines and their failure rate was not reviewed as part of this analysis but it also recommended if improved transportation packaging for the AV-OS machines does not result in a reduction of machine failures. Vibration, environmental effects and contamination are all likely to contribute to an increased machine failure rate.

Appendix M - AccuVote Functional Test Guidelines

1. Introduction

The purpose of this document is to outline a set of recommended functional tests to be performed as part of pre-election and precinct testing for each AccuVote Optical Scan (AV-OS), AccuVote Touchscreen (AV-TSX) machine, Voter Card Encoder and GEMS server in preparation for deployment during an election cycle.

This document is organized into two sections. The first, "Current Functional Tests" outlines the current functional tests performed by the Division of Elections prior to deployment of the AV-OS, AV-TSX, and Voter Card Encoder devices in each precinct for an election cycle. The second section "SOAESP Recommended Functional Tests" details an expanded set of functional tests recommended for implementation. This expanded set of functional tests provides a more comprehensive functional check prior to each election cycle potentially reducing the number of election system failures in the field on election day.

2. Current Functional Tests

Currently the Division of Elections performs functional testing on the AV-OS platform prior to deployment for each election cycle. The AV-TSX platform is subjected to Logic and Accuracy testing but documentation received by the SOAESP project team does not indicate functionality testing before each election cycle. In addition, no documentation indicates functional testing on the Voter Card Encoder or GEMS server election system components. Section 3 of this document outlines recommended functional tests for these components.

2.1 AV-OS Physical Test

2.1.1 Physical damage to unit check.
The AV-OS machine is physically inspected for damage prior to use. Specific damage to identify is not called out in the test procedure.

2.1.2 Printer door lock test
The door lock to the AV-OS printer compartment is checked to ensure that the lock is functional and that the key works in the lock.

2.1.3 Serial number or State of Alaska tag number recording
The serial number or State of Alaska tag number is recorded at the top of the functional test document.

2.1.4 LCD readability test
The AV-OS is tested to qualitatively confirm that the LCD is readable and that the entire LCD component has not failed.

2.2 AV-OS Vote / Modem Testing (Regional Offices)

In addition to the physical test set specified by the Division of Elections an additional set of tests focused on verifying modem connectivity between the AV-OS and the GEMS is also conducted.

Upon startup of the AV-OS in pre-election mode the AV-OS supervisor or central administrator follows a set of prompts within the system to perform a series of tests on the AV-OS machine.

Test Ballots

The AV-OS vote test verifies that the ballot counting functionality is working properly. This test does not include the validation of un-voted or fully voted ballots. Upon completion of the ballot count test the user instructs the AV-OS system to print the test results in short form.

Modem Transmission Test

The user follows the LCD prompts, validates the phone number in the AV-OS and transmits the results by telephone to the modem bank connected to the GEMS server in the Juneau Division of Elections director's office. The AV-OS transmits the dummy data and the modem transmission test is completed.

Comments

The Vote / Modem Testing procedure currently in use by the Division of Elections provides a very basic functional check of two portions of the AV-OS system. These checks confirm ballot counting (not tabulation) and modem functionality.

The AV-OS system provides a suite of tests that should be considered by the Division of Elections to decrease the probability of discovering a failed component or system on the AV-OS machine on election day. We recommend a test suite for consideration by the Division of Elections detailed in Section 3 of this document.

3. SOAESP Recommended Functional Test Procedure

3.1 Election Functional Test Lifecycle

The recommended functional tests are broken into two different groups. A set of functional tests is recommended to be performed at the Regional Center prior to precinct shipment. Upon arrival at the precinct it is recommended that a subset of these test be re-performed to ensure reliable functionality on voting day.

Precinct tests are intended to be performed at the precinct immediately prior to the election and their purpose is to validate the hardware for use on election day. The Regional Office tests are more comprehensive and are intended to identify any issues with a machine before it is distributed to the precinct for use in the election.

A checklist should be provided to each Regional Center. This checklist (similar to the one currently in use by the Division of Elections) would be filled out and returned with the AV-OS machine at the end of the election. Anomalies or comments should be included on the

checklist sheet to identify any issues arising from the tests. Each checklist should be scanned at the end of the election and logged electronically to a common location for each machine to create a functional checkout history of the machine.

A sample functional test lifecycle for AV-OS and AV-TSX machines is provided below.

1. Election cycle checklist is generated for each voting machine (AV-OS and AV-TSX).
2. Functional testing is performed for each AV-OS and AV-TSX machine at the Regional Center level. (This does not necessarily imply that the test itself must be performed physically at the Regional Center).
3. The functional test checklist document is filled out by the Regional Center level technician.
4. The AV-OS or AV-TSX machine is boxed and readied for shipment with the functional test checklist included in the box.
5. Functional testing is performed for each AV-OS or AV-TSX machine at the Precinct level prior to election administration for each election (Primary and General). The functional test checklist document is further updated with the results of the precinct level test for the Primary and General elections.
6. The election is conducted.
7. The functional test checklist document and AV-OS or AV-TSX machines are re-packaged and returned to Division of Elections officials.
8. The functional test checklist documents are collected and scanned for historical purposes. Backed up electronic storage should be used to maintain the integrity of the functional checklist documentation.

A functional check of the Voter Card Encoder devices is recommended prior to each election. A complete history of the Voter Card Encoder functional testing is not recommended at this time.

GEMS functional testing is recommended on a per election basis and it is further recommended that the test documentation be archived in manner similar to that suggested for the AV-OS and AV-TSX machines. A sample GEMS functional test lifecycle is presented below.

1. Election cycle checklist is generated for each election system GEMS.
2. Functional testing is performed on each GEMS machine prior to the administration of the election.
3. The functional test checklist is completed by the test technician and is returned to the appropriate individual for historical archiving. Any anomalies or inconsistencies are noted in the functional test checklist form and are thus permanently recorded.

3.2 AccuVote Formatting and Clearing Procedure

The AccuVote system stores election ballots and vote tabulation data on a variety of different media during the process of an election. It is desirable from a security standpoint to clear and re-format the electronic storage media prior to use during each election cycle. Two different Election Management models were developed by Premier Election Solutions in response to the State of California de-certifying the Diebold equipment for use in California. It is recommended that the Division of Elections implement the Air Gap Election Management model as presented in Premier Elections Solutions document Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007).

3.2.2 GEMS Server Configuration

The Air Gap election management model requires the use of three separate host computers and maintains integrity and security by limiting the operations performed on each computer platform. The purpose of each computer is summarized below.

GEMS Server 1: GEMS server 1 is used to create election definitions, ballot templates and to download data to the voting machine memory cards.

GEMS Server 2: GEMS server 2 is used to capture uploaded election results from the AV-TSX and AV-OS precinct machines.

Workstation Computer: The workstation computer (more than one is possible) is used to clear the contents of AV-TSX memory cards prior to re-use in the AccuVote election system. The workstations used for this purpose should be dedicated to memory card storage clearing and should be minimally configured.

See Section 3.2 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007) for more information

3.2.3 AV-TSX PCMCIA Memory Card Storage Clearing

The contents of the AV-TSX memory cards should be cleared prior to each election cycle. The workstation computer(s) should be used to reformat the contents of each PCMCIA memory card. See Section 4.4 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007)

3.2.4 AV-OS Memory Card Storage Clearing

The contents of the AV-OS memory cards should be cleared using an AV-OS machine prior to each election cycle. See Section 4.5 of Plan on Formatting and Clearing Program Storage on Voting System, Revision 1.0 (2007) for details on the AV-OS memory card clearing procedure.

3.3 AV-OS Regional Center Tests

In addition to the existing functional tests specified by the Division of Elections (see Sections 1.1 and 1.2), the following additional tests and / or actions are recommended for each election cycle.

The majority of the tests or actions listed below require Diagnostics Mode access to the AV-OS machine.

3.3.1 Key Functionality Check

Locate all AV-OS keys. The AV-OS system utilizes a key for printer access and a key for ballot box access. Verify that AV-OS printer key opens printer door. Verify that ballot box key opens security plate and all other ballot box access points to ensure key functionality.

3.3.2 Serial Number Recording

Record the hardware serial number of the AV-OS machine in the functional checklist document. This procedure ensures that the documentation associated with the test is associated with a specific AV-OS machine and traceability of the machine's life can be

maintained. The State of Alaska asset tag should also be recorded if it is present. The asset tag should not be used in lieu of the serial number but in addition to it.

3.3.3 Firmware Version Validation and Recording

Record the firmware version of the AV-OS machine. Validate the reported firmware version against the known correct version. Do not use AV-OS if reported firmware version does not match expected value.

3.3.4 System Clock Setting

Verify that the system clock is set. If the clock is not set properly follow the procedure in the AccuVote-OS user's guide to set the clock. The clock maintains the date and time in the AV-OS machine and is backed up by the system battery (Diebold Election Systems AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.2, 2005).

3.3.5 LCD Test

This test confirms that the AV-OS machine's LCD display can properly reproduce all of the required text characters (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.4, 2005).

3.3.6 System Memory Test

This test writes a set of test data to the AV-OS system memory and reads it back from the system memory. This test is successful if the data read is identical to the data written to system memory (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.5, 2005).

3.3.7 Memory Card Test – REQUIRES A BLANK AV-OS MEMORY CARD

This test writes a set of test data to the AV-OS memory card and reads it back from the memory card. This test is successful if the data read is identical to the data written to the memory card (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.6, 2005).

3.3.8 Printer Test

This test is executed during the Memory Card Test and validates the printer functionality by printing a subset of the standard character set on the printer tape (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.6, 2005).

3.3.9 Auxiliary Serial Port Test

This test confirms that the modem interface is functional to ensure that election results can be properly transmitted upon election close. This is an internal test and does not require a connection to the Public Switched Telephone Network (AccuVote-OS Precinct Count 1.96 User's Guide Revision 4.0, Section 17.8, 2005).

3.3.10 Card Reader Test

This test confirms that the optical scanning read sensor channels (34 total on each ballot side) are functioning properly. It is not recommended to perform the card reader test using the "RECIRCULATE BALLOTS?" mode.

3.4 AV-OS Precinct Tests

The precinct testing involves a subset of the Regional Center level testing. The purpose of the precinct level testing is to confirm that the machine is not physically damaged and to detect high level problems with the AV-OS machine.

1. Physical Damage Inspection (see Section 2.1.1)
2. Serial Number Recording (see Section 3.2.2)
3. Firmware Version Validation and Recording. (see Section 3.2.3)
4. Key Functionality Check (see Section 3.2.1)

3.5 AV-TSX Regional Center Tests

The following tests are recommended to be performed at the regional center before an AV-TSX voting machine is distributed to a precinct for use in an election.

3.5.1 Physical Damage Inspection

The AV-TSX machine is inspected for physical damage during shipment or setup. All tamper-evident seals are checked to confirm that the AV-TSX machine has not been compromised. The security hologram is inspected during the physical damage inspection.

3.5.2 Machine Serial Number Validation

The AV-TSX hardware serial number is recorded on the checklist functional test sheet. Once the machine has booted, access the software reported serial number from the settings menu and confirm that the physical serial number and the software serial number match (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.1.1, 2005)

3.5.3 Hardware and Firmware Version Validation

The AV-TSX Bootloader version, Windows CE version and BallotStation versions are checked and recorded during AV-TSX system boot after power is applied to the machine.

3.5.4 Card Reader Port Validation

This test confirms that the smart card reader can perform the required read / write operations without error (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.1.2, 2005).

3.5.5 Date and Time Programming

This procedure sets the date and time in the AV-TSX machine (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.2, 2005).

3.5.6 Screen Display Calibration

This procedure calibrates the touchscreen and ensures that voter selections match with the software display presented to the user (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.3.2, 2005).

3.5.7 Printer Test

This test ensures that the AV-TSX VVPAT printer can printer the required paper ballot without error (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.4.1, 2005).

3.5.8 Audio Test

This test ensures that the audio output subsystem of the AV-TSX machine is operational (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.7, 2005).

3.5.9 Modem Test

This test validates the AV-TSX internal modem functionality and confirms the AV-TSX's ability to send data to the internal modem (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.9, 2005).

3.5.10 Security Setting Validation

This procedure validates the security settings of the AV-TSX for use in the election. The security setting validation procedure should include certificate validation and key signature validation. It may be desirable to implement the Key Card Tool key update procedure during this functional test step (Ballot Station 4.6 Users Guide Revision 2.0 Section 8.3.10, 2005)

3.5.11 Central Administrator / Supervisor Access Test

A valid central administrator card and a valid supervisor card should be inserted into the AV-TSX machine following the Key Card update to ensure that central administrator access is available. An invalid central administrator and an invalid supervisor card should be inserted into the AV-TSX machine following the Key Card update to ensure that the security keys are properly transferred and the AV-TSX machine has been secured.

3.6 AV-TSX Precinct Tests

The precinct level tests for use with the AV-TSX are a subset of the regional center tests. The recommended suite of precinct tests is given below.

3.6.1 Physical Damage Inspection (see Section 3.4.1)
3.6.2 Machine Serial Number Validation (see Section 3.4.2)
3.6.3 Hardware and Firmware Version Validation (see Section 3.4.3)
3.6.4 Printer Test (see Section 3.4.7)
3.6.5 Supervisor Access Test (see Section 3.4.11)

3.7 Voter Card Encoder Tests

The Voter Card Encoder is used to create valid voter cards for use in the AV-TSX machines. Each Voter Card Encoder device should be tested prior to use in a precinct for voting during an election.

3.7.1 Voter Card Encoder Physical Damage Check

Inspect the Voter Card Encoder for visible physical damage.

3.7.2 Voter Card Encoder Display Check

The Voter Card Encoder should be powered on and the display should be checked to ensure that it is visible and all characters are visible. Fading should not be evident on the LCD display.

3.7.3 Voter Card Encoder Firmware Check

This procedure checks the Voter Card Encoder firmware level and ensures that the proper revision of firmware is present on the Voter Card Encoder.

3.7.4 Voter Card Encoder Supervisor Access Check

Supervisor access to the Voter Card Encoder should be verified.

3.8 GEMS Server / Workstation Tests

The AccuVote GEMS server is used to create election definitions, ballot templates and to download data to the voting machine memory cards as well as to receive uploaded precinct results from AV-TSX and AV-OS machines. Use of the Air Gap Election Management model (see Section 3.2) requires implementing two GEMS servers for each election. Both GEMS servers should have functional tests performed prior to use during an election cycle. A third workstation is used to wipe AV-TSX memory cards prior to election programming.

3.8.1 GEMS BIOS (Built-in Operating System) Password Validation

The GEMS server should implement a BIOS password policy compliant with the password management plan (Appendix E – Physical Password Management Recommendations, 2008).

3.8.2 Verify System, Service Pack, Server Model, Processor, Disk Size and RAM Parameters

The GEMS server should have the system parameters listed above checked prior to use to ensure that tampering has not occurred on the system.

3.8.3 GEMS Software Hash Verification

The GEMS.exe application should be validated by calculating both MD5 (Message-Digest 5) and SHA (Secure Hash Algorithm) hash functions. These hash codes should be compared with those registered with the National Software Reference Library (http://www.nrsl.nist.gov/votedata.html). Known vulnerabilities exist with the MD5 hash function and as a result both the MD5 and SHA hash functions should be calculated (Premier's Windows Configuration Guide, Revision 3.0, Section 10, 2007).

3.8.4 Loaded Software Confirmation

The GEMS server should be checked to ensure that only Winzip v11, Adobe Acrobat 8, Adobe Audition 2.0 or Sony SoundForge 8 and Nero Burning ROM 8 are the only applications loaded on the server.

3.8.4.1 GEMS Operating System Update Packages Validation

The GEMS server should have the recommended operating system update packages installed (Premier's Windows Configuration Guide, Revision 3.0 Section 4, 2007).

3.8.4.2 GEMS Operating System Services Validation

The GEMS server should have the recommended services running (Premier's Windows Configuration Guide, Revision 3.0 Section 5, 2007). All other system services should be disabled.

3.8.4.3 GEMS Operating System Data Execution Protection Module Validation

The GEMS server should have the Data Execution Protection (DEP) modules turned on as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 6 (2007).

3.8.4.4 GEMS Operating System Security Policy Validation

The GEMS server should have security policies validated which are in compliance with the SOAESP recommended password policy and which are compliant with Premier's Windows Configuration Guide, Revision 3.0, Section 7 (2007).

3.8.4.5 GEMS Server File Permission Validation

The GEMS server file permissions should be assigned as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 8 (2007).

3.8.4.6 GEMS Operating System Registry Permission Validation

The GEMS server registry permission should be assigned as indicated in Premier's Windows Configuration Guide, Revision 3.0, Section 9 (2007).

3.8.5 GEMS Server Date and Time Adjustment

The date and time on the GEMS server should be set to the current values prior to use during an election.

3.8.6 Network Address Validation

The network address reported by the GEMS server should be checked prior to use to ensure that it is NOT connected to a network.

3.8.7 GEMS Acceptance Test Database Test

The GEMS acceptance test database should be loaded and the contents of the test database validated using the GEMS software.

3.8.8 GEMS Database Backup

The GEMS database backup functionality should be confirmed prior to use of the GEMS software for election management. Ensure that a backed up database file can be properly read into the GEMS software.

3.8.9 GEMS Print Test

The GEMS printing functionality should be validated by initiating an “Administrative Report” from within the GEMS software. Both the hardware printer driver and the pdf printer driver should be tested.

3.8.10 Key Card Tool Test

A dedicated Key Card Tool workstation should be used to perform the Key Card Tool test. This workstation should be used to generate new security keys on a smart key card. The keys loaded on the smart key card should be confirmed by removing the card and then reading the keys back into the Key Card Tool software.

4 Recommendations

It is recommended that the Division of Elections implement all of the recommended tests presented in this document in addition to the tests already being used. The addition of the tests detailed in this document provides a more comprehensive functional check out of the system and reduces the potential problems encountered on election day. Adoption of the historical logging of checklist documentation ensures that the lifecycle of each voting machine is documented and available for review at a later time.

Appendix N - AccuVote Logic and Accuracy Guidelines

1 Introduction

The logic and accuracy guidelines presented here establish a minimum set of requirements to confirm that each electronic voting machine is producing reliable, accurate results.

This document is organized by first presenting the currently implemented logic and accuracy procedures in use by the Division of Elections. Following the currently implemented procedures a set of additional recommendations is presented which is intended to enhance the output of the logic and accuracy testing.

2 Current Logic and Accuracy Procedures

2.1 AccuVote Optical Scan (AV-OS)

The AV-OS machines are tested for logic and accuracy using a test deck of ballots with known results. The logic and accuracy test is implemented by shuffling the test ballot deck to create a randomly oriented set of ballots. The user then verifies that the number of ballots fed into the AV-OS machine matches that reported on the AV-OS public LCD. The results of the test deck are printed in short form. The results printed on the AV-OS results tape are compared with the known outcome.

The AV-OS machine's memory card is then prepared for the election and the machine is powered off until the actual election is conducted.

2.2 AV-TSX

The AV-TSX are tested for logic and accuracy by following a procedure designed to identify election programming errors. This procedure first clears results that are already present on the memory card. The technician then prints a zero totals report to ensure that the results memory register of the memory card was cleared.

Once the memory card results register is cleared the technician then creates a voter access card for each ballot type being tested. Manual test mode is used (requiring voter access cards) to perform the logic and accuracy testing for each ballot type in the election. Once all of the ballot types have been voted the results are printed and reviewed to ensure that the voted values match the expected results. Once the logic and accuracy of the printed results is review the memory card is set to election mode and is physically removed from the AV-TSX machine.

2.3 GEMS

Currently no explicit logic and accuracy testing is performed by the Division of Elections.

3 Recommended Logic and Accuracy Procedures

3.1 AV-OS

The AV-OS logic and accuracy testing procedure presented here ensures that the logic of the ballot programming is correct and that votes cast in each oval position are accurately tabulated.

In order to perform the AV-OS logic and accuracy tests several sets of test ballots must be prepared corresponding to each ballot type to be used in the election. The following sections describe the three different test decks to be used for AV-OS logic and accuracy testing.

3.1.1 LAn Test Deck Test

The LAn (Logic and Accuracy for n candidates) test deck test validates that all candidates in all races and on all ballots are counted correctly. In the LAn test a test ballot is created for each possible contest where the voting outcome is produced as shown below (where n = 5):

Race 1 Test Deck	
Candidate	**Vote Count**
A1	1
B1	2
C1	3
D1	4
E1	5

Ballot 1	
Candidate	**Vote**
A1	X
B1	
C1	
D1	
E1	

Ballot 2	
Candidate	**Vote**
A1	
B1	X
C1	
D1	
E1	

Race 2 Test Deck	
Candidate	**Vote Count**
A2	1
B2	2
C2	3
D2	4
E2	5

Ballot 3	
Candidate	**Vote**
A1	
B1	X
C1	
D1	
E1	

Ballot 4	
Candidate	**Vote**
A1	
B1	
C1	X
D1	
E1	

The race tabulations above show the number of tabulated votes for Races 1 and 2. The sample ballots shown are the first four ballots in the test deck for race 1. A total of 15 ballots would be required for each race shown.

A test ballot deck should be produced for all races for each ballot style.

3.1.3 Multi-vote Test Deck

The multi-vote test deck is used for ballots where “vote for more than one” races are programmed. In these races the ballots should be filled out as follows.

3.1.3.1 Overvote Ballot

The overvote ballot contains one more oval on each “vote for more than one” race than is allowed by the election program. The sample ballot shown is for a “Vote for Three” race where 4 ovals were selected.

Overvote Ballot	
Candidate	**Vote**
A	X
B	X
C	X
D	X
E	

3.1.3.2 Test Ballots

The test ballot deck for the multi-vote case consists of ballot as shown below (Vote for 3 ballot with 5 candidates):

Multi-vote Ballot 1	
Candidate	**Vote**
A	X
B	X
C	X
D	
E	

Multi-vote Ballot 2	
Candidate	**Vote**
A	
B	X
C	X
D	X
E	

Multi-vote Ballot 3	
Candidate	**Vote**
A	
B	
C	X
D	X
E	X

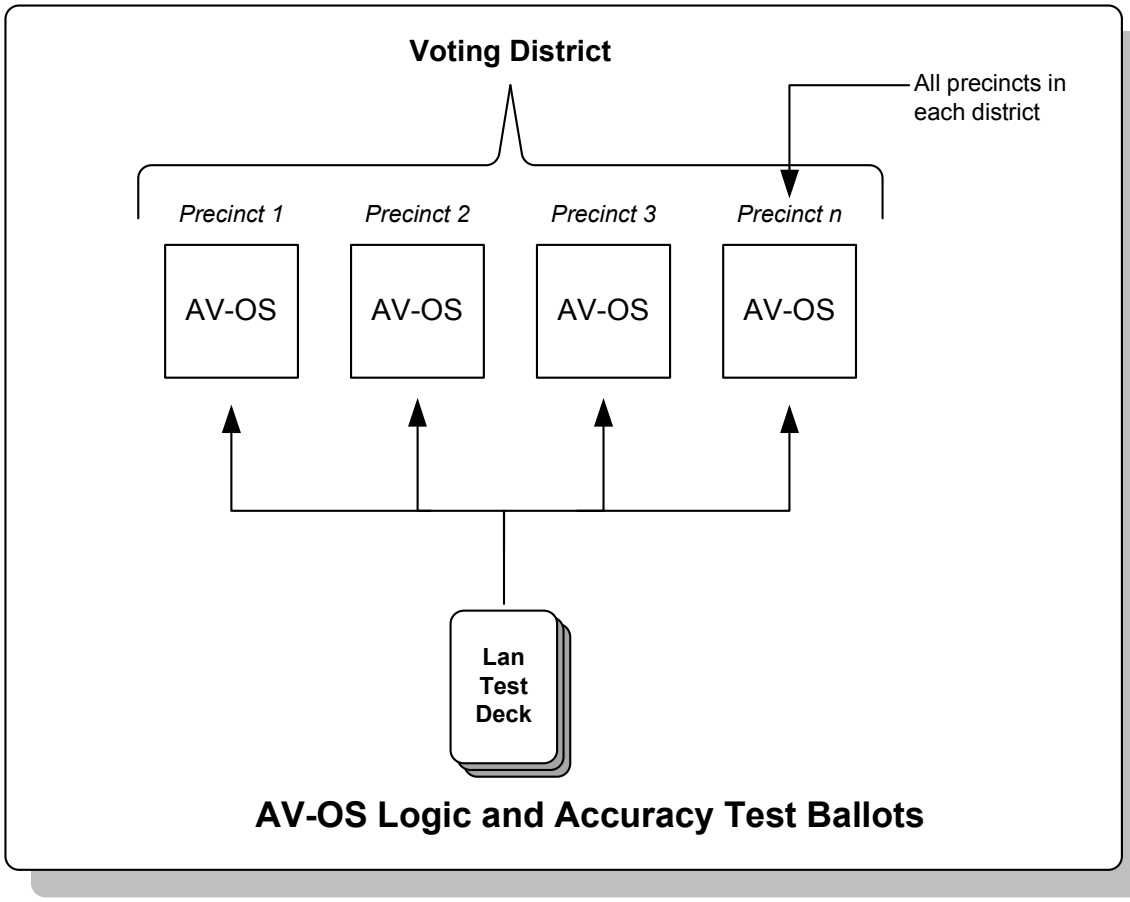
Multi-vote Test Deck	
Candidate	**Vote Count**
A	1
B	2
C	3
D	2
E	1

3.1.4 Logic and Accuracy Test Procedure

The logic and accuracy test should be performed on all AV-OS machines that will be used in the election. Following each test a precinct results tape should be printed and the results compared with the expected outcome. The results of the test should be uploaded to the GEMS and reports on the GEMS server should be generated which confirm the expected outcome.

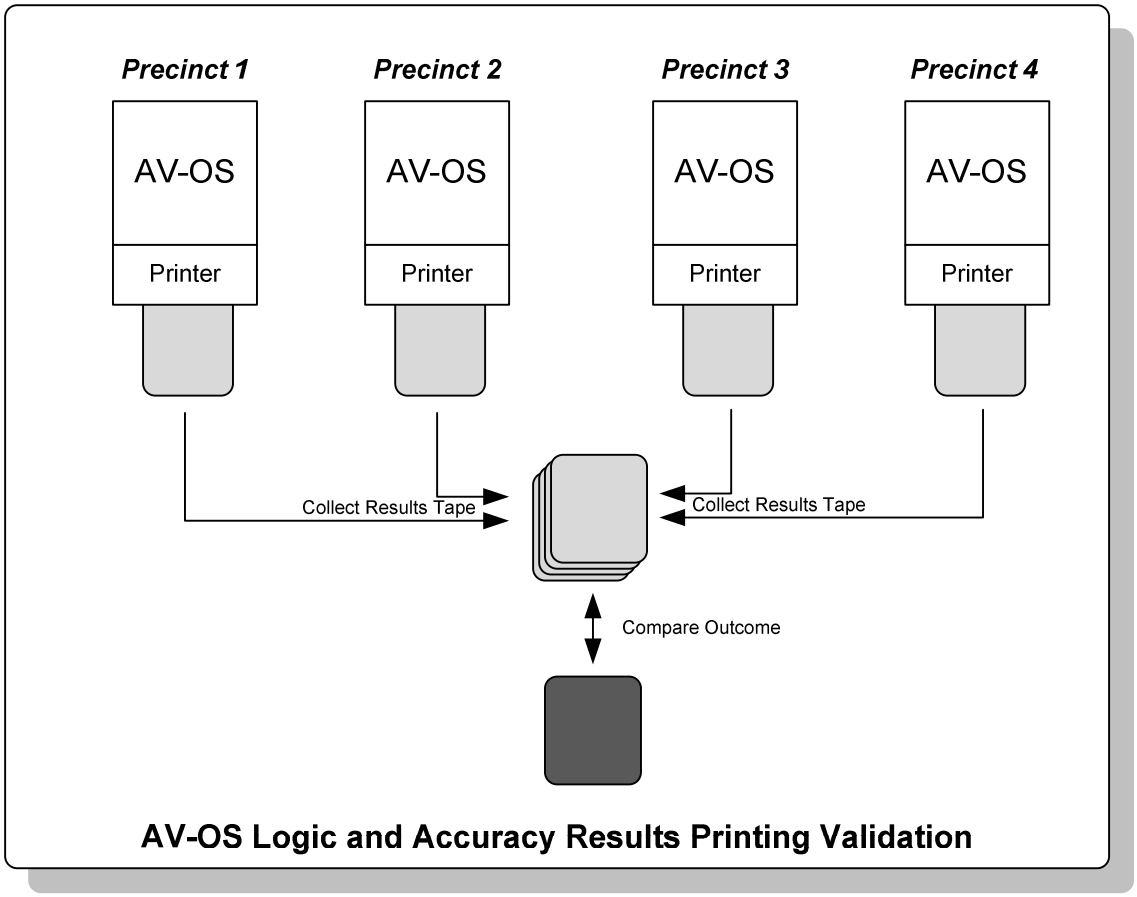
Logic and accuracy testing for the AV-OS system should be conducted by following the procedure below.

1. Run a LAn test deck through the AV-OS machine for every ballot style that will be used in the AV-OS machine.



LAn test ballots are run through every AV-OS in each voting district.

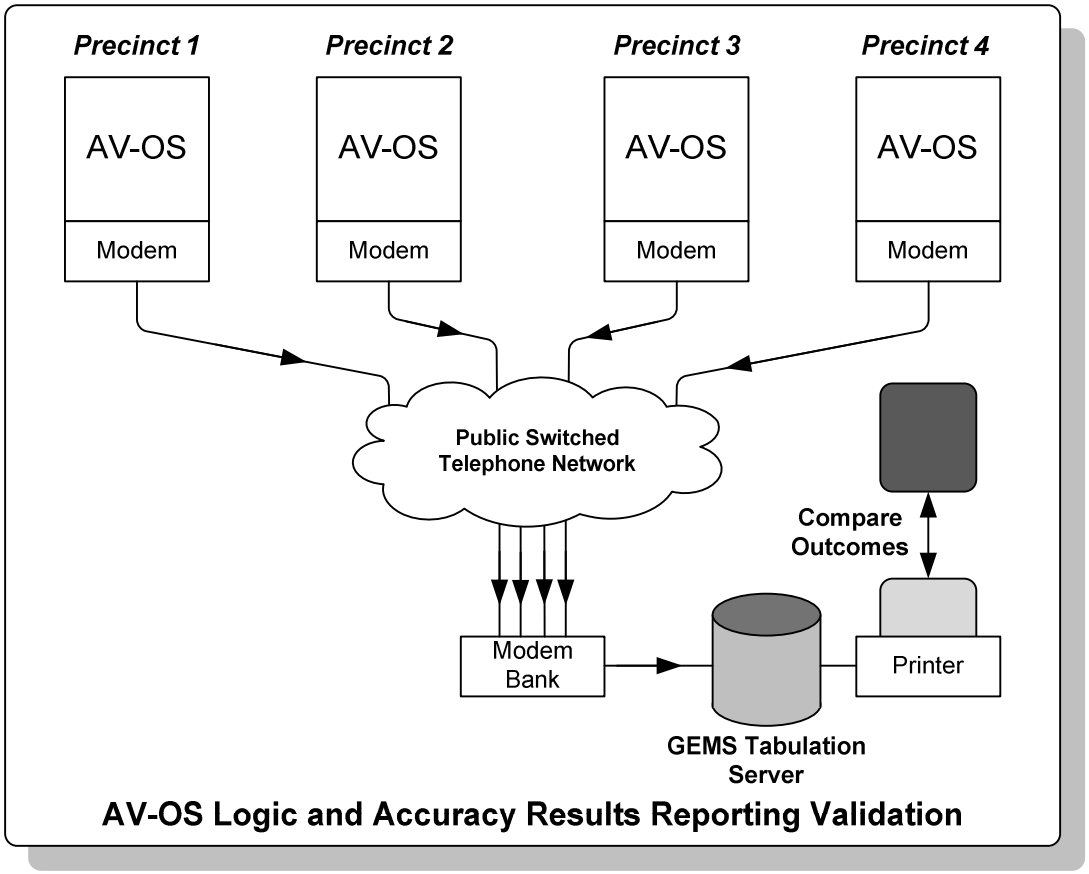
2. Print the results tape and confirm that the results match the expected value.



AV-OS Logic and Accuracy Results Printing Validation

Each AV-OS machine prints a results tape and these results tape outcomes are compared with the known expected outcome to ensure that tabulation is occurring accurately.

3. Transmit the results to the GEMS server.
4. Following the transmission of all results to the GEMS server a report is generated and the contents are compared with the expected value for the test ballot results.



5. The paper ballot decks generated for the use in the logic and accuracy tests as well as the logic and accuracy printed results should be archived together for historical purposes. Scanning of the results and electronic storage of these logic and accuracy test results is recommended.

3.2 AV-TSX

The AccuVote Touchscreen Ballot Station software offers the user two different approaches for logic and accuracy testing. These approaches are labeled Manual and Automated within the Ballot Station software.

3.2.1 Manual Logic and Accuracy Testing

In Manual Logic and Accuracy testing the user manually casts a series of test ballots to validate that the AV-TSX is properly counting ballots. The Premier recommended AV-TSX manual logic and accuracy test is performed by selecting the manual logic and accuracy test option within the Ballot Station software. The

manual test automatically casts a successively increasing number of ballots until the number of ballots is equal to the number of candidates in the largest race.

3.2.2 Automated Logic and Accuracy Testing

The AV-TSX Ballot Station software includes an option for automated logic and accuracy testing. In the automated test environment the tester selects a pre-determined combination of ballots to be voted. The system automatically casts the ballots and tabulates the results. The number of ballots cast is increased on each iteration until the number of ballots equals the number of candidates in the largest race on the ballot (as in the manual test mode). Additionally, a blank ballot is cast for each ballot set.

The tester can select from 5 different ballot testing options within the automated test mode. It is recommended that the test technician perform the Full Test by Ballot and the Full Test by Precinct automated tests.

The Ballot Station software offers two options while performing the automated test procedures. The *Use Ballot Rotation* option allows the user to rotate the candidate position. The *Provisional Ballots* option allows the user to specify the use of provisional ballots during the test.

3.2.2.1 Full Test by Ballot

The full test by ballot test votes a full set of ballots for every ballot on the memory card. Each unique ballot on the memory card is voted by casting votes as shown below.

AV-TSX Full Test by Ballot	
Candidate	**Vote Count**
A	1
B	2
C	3
D	4
E	5
Total Ballots	15

This procedure is iterated until all unique ballots on the memory card have been voted.

3.2.2.2 Full Test by Precinct

The full test by precinct test casts a full set of ballots for every base precinct present on the memory card. Ballots are cast in the same manner as shown in section 3.2.2.1 where the number of ballots cast is increased on each iteration until the number of ballots cast is equal to the largest number of candidates in that race.

3.2.3 Results Validation

3.2.3.1 Print Results

Once the logic and accuracy tests are completed it is recommended that the results be printed and the results on the printed tape be validated against the expected results.

3.2.3.2 Upload Results

The results of the logic and accuracy test should be uploaded to the GEMS server using the internal modem. Once the results have been uploaded an election report should be printed and validated against the expected results.

3.3 GEMS

3.3.1 Tabulation Accuracy Validation

The GEMS host computer in the Director's office in Juneau is used to tabulate logic and accuracy results transmitted during the logic and accuracy testing of each machine. The GEMS Summary, Statement of Votes Cast and the Cards Cast report results must be reconciled with the results obtained in the AV-OS and AV-TSX machines (GEMS 1.18 Election Administrator's Guide, 2006).

4. Recommendations

We recommend that the Division of Elections implement all of the tests presented in this document in addition to the tests already in use. The increased scope of the tests detailed here provides a more comprehensive validation of the logic and accuracy of the programmed election. Detailed documentation of the test results for each AV-OS and AV-TSX machine is recommended for each election cycle. Historical logging of these results is also recommended in electronic format.

Appendix O - AccuVote Touchscreen

Smart Key Card Enhancement Options

1. System Description

The AccutVote Touchscreen voting system is comprised of several different components. System security is maintained by utilizing a suite of smart cards to secure the election ballot, vote tallies, the touchscreen voting machine operating system, and other sensitive system data. The smart card system is comprised of four different smart cards, the Key Card Tool application and a smart card programmer.

This section describes each system component in the context of the key card tool application. Each component is described along with its interaction with the key card security implementation.

Key Card Tool Software

Key Card Tool is a software application created by Premier Election Systems for use with the AccuVote Touchscreen (AV-TSX) system. The Key Card Tool application allows users to create authentication keys and passwords on a personal computer platform and to write those authentication keys to smart cards for use in the touchscreen voting system.

Key Card Tool requires a personal computer workstation on which the Key Card Tool application runs as well as a smart card reader which interfaces to the personal computer communications port. The smart card reader is used to read and write authentication keys and passwords to individual smart cards.

Smart Key Card

The smart key card is the basis of the touchscreen system access security. The smart key card stores two authentication keys and two passwords. The smart card key is used to authenticate user access at the central administrator, supervisor and voter levels. The smart card key validates the user's authentication key against the key present in the hardware device being accessed. The data key is used to encrypt individual data files within the ballot station (firmware that operates on the touchscreen terminal). A password is stored to secure central administrator access and another is stored to secure supervisor access to the touchscreen machine.

The smart key card is programmed by Premier with default values for the security and data keys as well as the central administrator and supervisor passwords. These passwords are well known in the public domain and are considered insecure. Replacement of the key and password values is accomplished through the use of the Key Card Tool application.

The Key Card Tool application allows the user to select new values for the security key, data key, central administrator password, and supervisor password and to write these values onto a blank smart card.

Once the central administrator and supervisor smart cards have been updated with new keys and passwords these cards cannot be further updated without the use of the Key Card Tool application and the original security keys.

After the smart key card has been programmed with the values selected by the election officials, the card is removed from the programming device and must be used to update the authentication keys on the touchscreen devices and the voter card encoder devices.

Central Administrator and Supervisor Cards

The central administrator and supervisor cards are used to secure central administrator and supervisor access to the AccuVote Touchscreen machine. Central administrator access allows users an expanded set of system options within the AccuVote Touchscreen system not available to users with supervisor or voter access. Supervisor access allows election administrators to open and close elections, print paper records and to transmit election results to the GEMS.

Central administrator and supervisor cards must be updated using the Key Card Tool application at any time the keys and passwords are changed. The cards are updated by inserting the smart card into the card encoding device and following the software procedure after the smart key card has been created.

Central administrator and supervisor touchscreen device access is obtained by inserting the central administrator or supervisor card into the touchscreen device and entering the appropriate password. Upon insertion of the smart card the card security key is authenticated against the terminal key and the user is granted the appropriate level of access. A central administrator or supervisor card that does not have valid security and data keys will be rejected by the system. After 7 unsuccessful attempts at system access using a smart card with invalid keys the smart card will be permanently disabled.

Voter Access Card

The voter access card is used to allow voters to cast their votes on the electronically defined ballot. The voter access card is programmed by a voter card encoder that is under the authority of election administrators. The voter card encoder must be updated with the security and data keys when the key and password values are updated. Voter cards are not required to be programmed by the Key Card Tool application.

During an election after election officials determine that a voter is allowed to cast a ballot the vote card encoder is used to enable a voter card. The voting process of an individual voter proceeds as follows:

1. An election official creates a valid voter access card by inserting a default voter access card into the voter card encoder.
2. The voter takes the valid voter access card to a touchscreen terminal and inserts it into the smart card slot. The system authenticates the voter access card against the authentication keys present in the AccuVote system software.
3. The voter casts a ballot and completes the voting process.

4. The AccuVote system software overwrites the voter access card authentication keys with default values defined by Premier.
5. The voter removes the voter access card and returns it to an election official.
6. The process is restarted using the voter access card with default security key values.

Voter access cards with previously assigned or invalid authentication keys cannot be used to cast a ballot on a terminal containing authentication keys which do not match the smart card keys.

2. Logistical Impact

Implementing the security enhancements available through the Premier Election Systems Key Card Tool product requires the State of Alaska Division of Elections to modify the manner in which it transports and stores the AccuVote Touchscreen devices.

Every authentication key and password change requires a system-wide AccuVote Touchscreen firmware authentication key update. This update includes:

1. Smart Key Card
2. Central Administrator Cards
3. Supervisor Cards
4. Voter Card Encoder
5. AccuVote Touchscreen Terminal

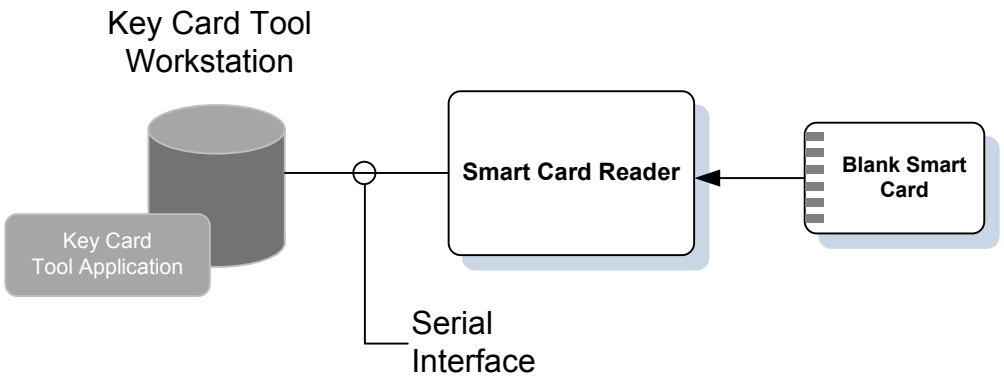
The system functions only when all hardware and software have the same authentication keys loaded.

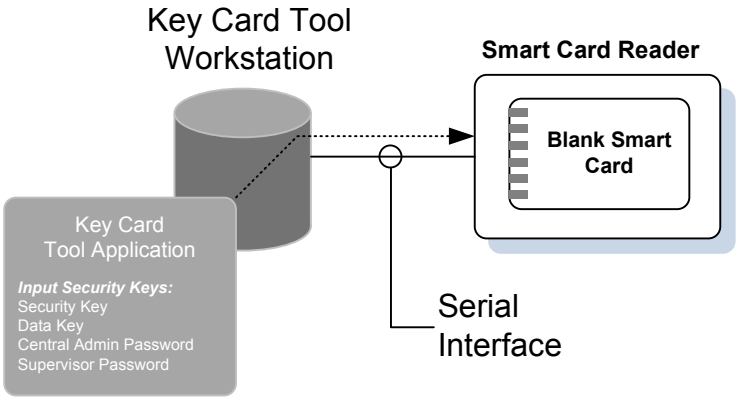
Currently the Division of Elections will ship AccuVote Touchscreen devices to remote communities for Primary elections. Upon completion of the Primary election the touchscreen terminals will remain in many remote communities until the general election some time later. This makes authentication key / password changes impossible during the “sleepover” period.

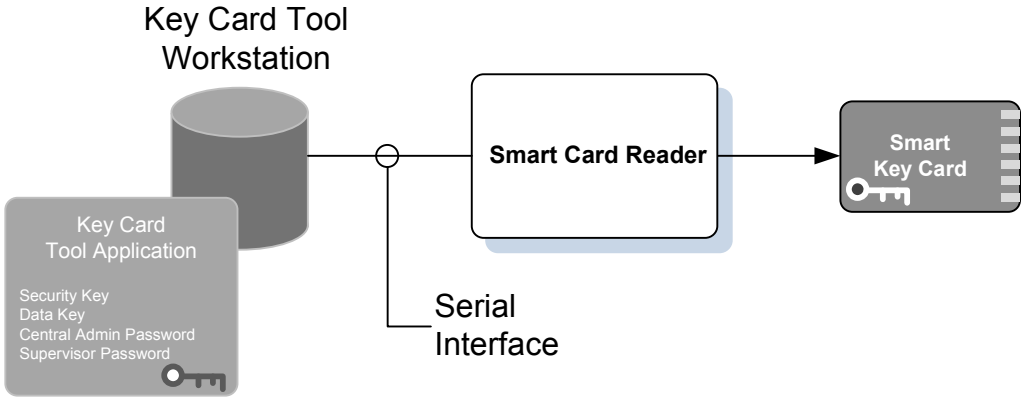
Implementing the highest level of security improvement in which the authentication keys / passwords are changed following each and every election requires the field equipment (touchscreen terminals and voter card encoders) to be returned to a central location for programming after the close of each election.

3. Recommendations

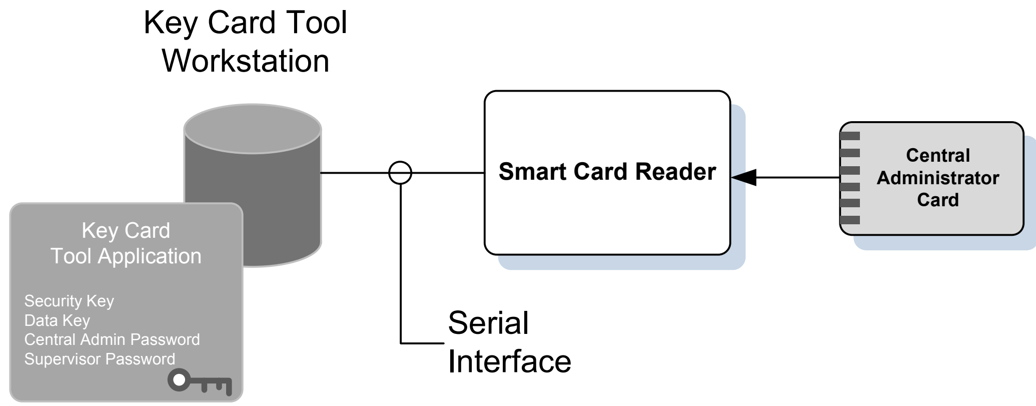
We recommend that the Division of Elections procure and implement the Key Card Tool application for use in the 2008 election cycle. We do not recommend returning the AV-TSX machines to have the encryption keys and passwords changed between the primary and general elections because of the significant logistical impact this would have on the Division of Elections. The use of the Key Card Tool application for each election cycle increases the security of the AccuVote Touch Screen system significantly.

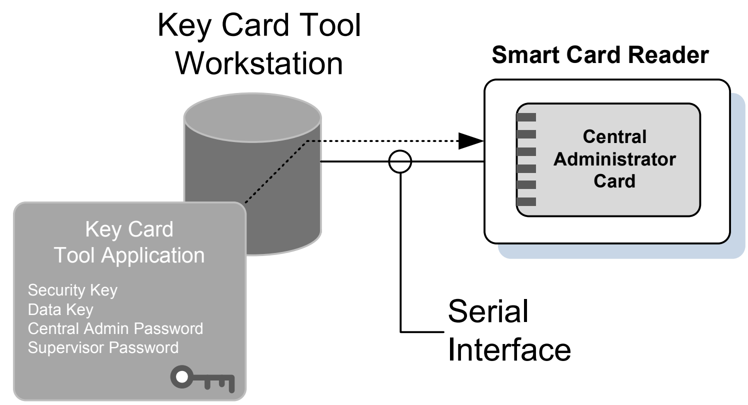


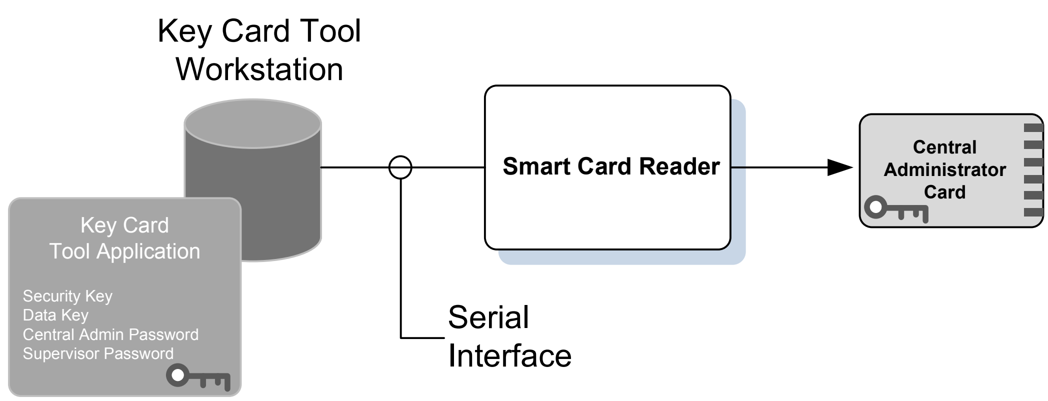




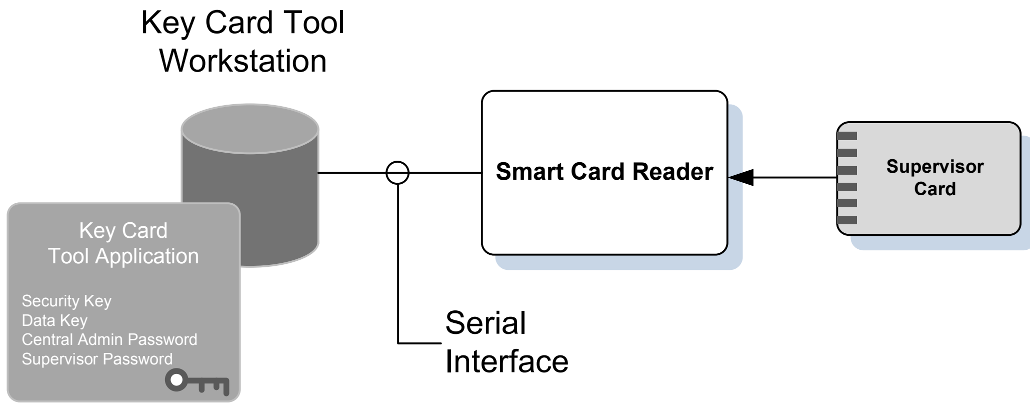
Premier Key Card Tool System Description			
Name:	Figure 1: Security Key Card Progamming		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	1 of 6

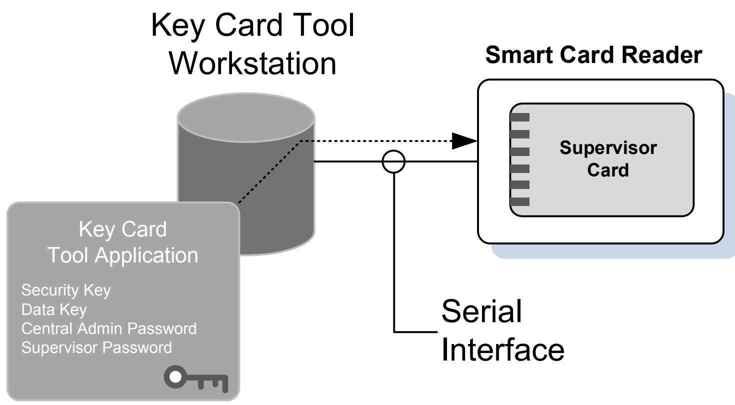


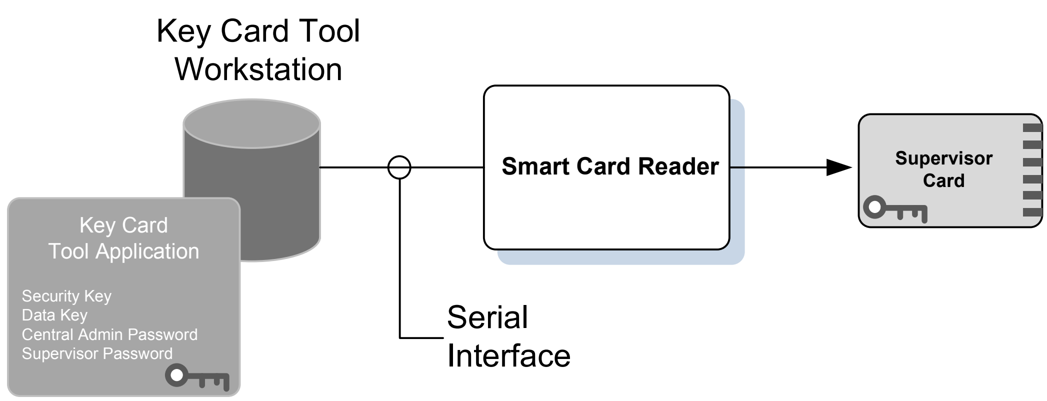




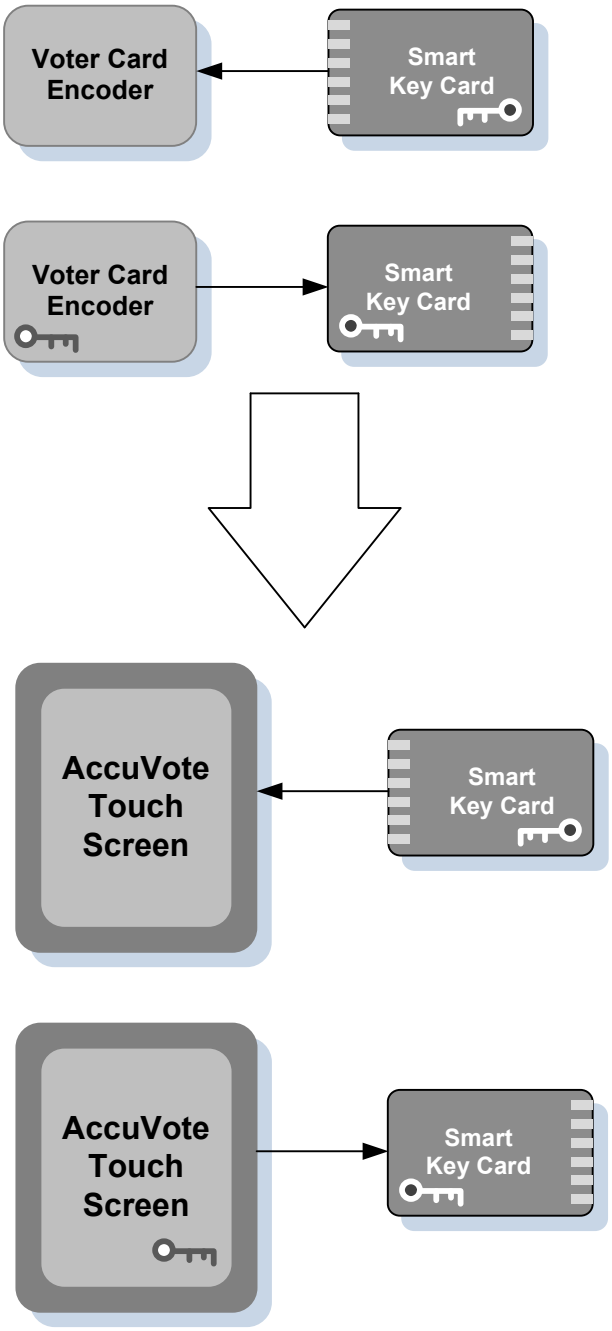
Premier Key Card Tool System Description			
Name:	Figure 2: Central Admin Card Programming		
Drawn By:	Mark Ayers	Date:	*4/15/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*2 of 6*



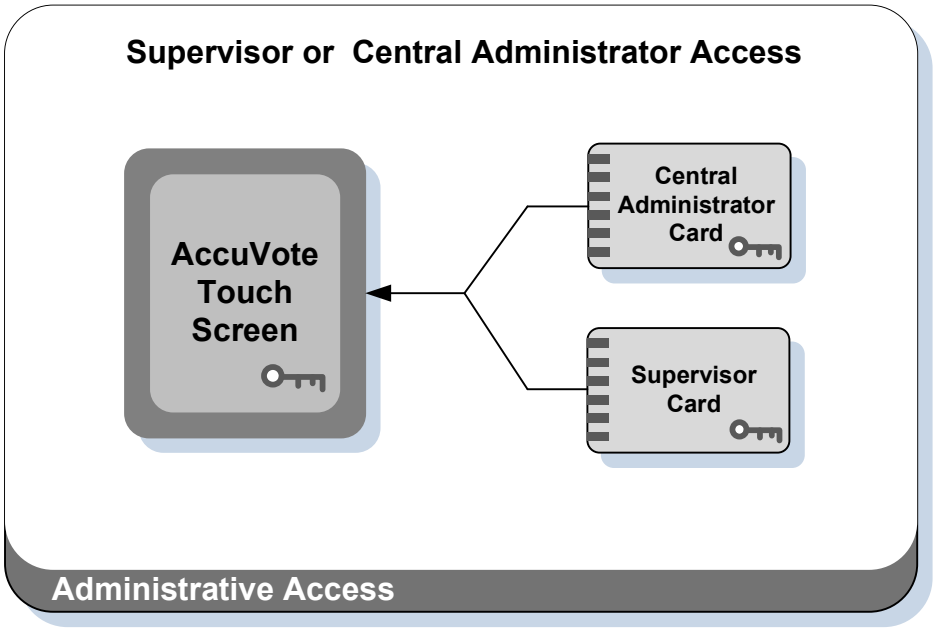


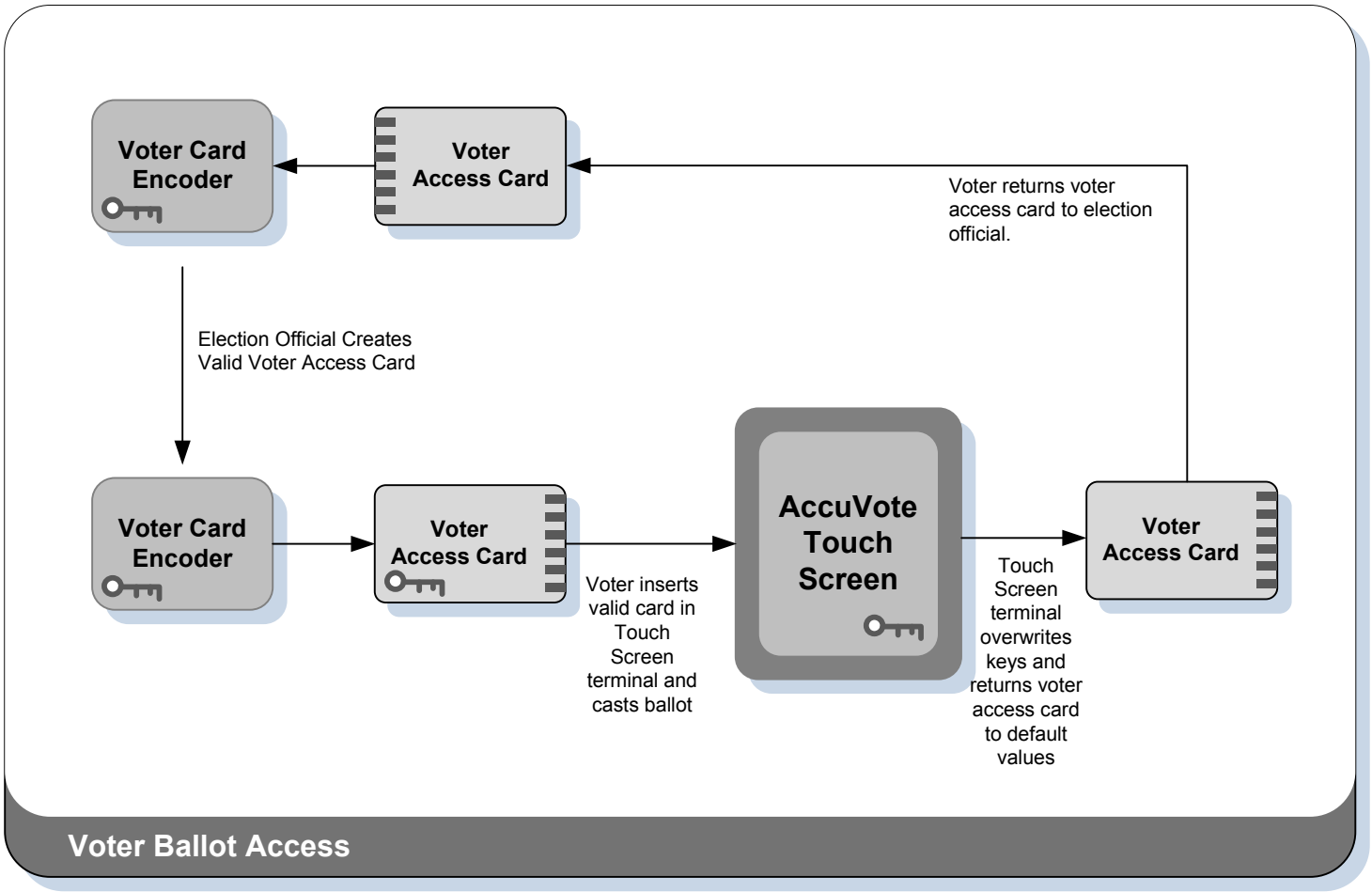


Premier Key Card Tool System Description			
Name:	Figure 3: Supervisor Card Programming		
Drawn By:	Mark Ayers	Date:	*4/15/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*3 of 6*

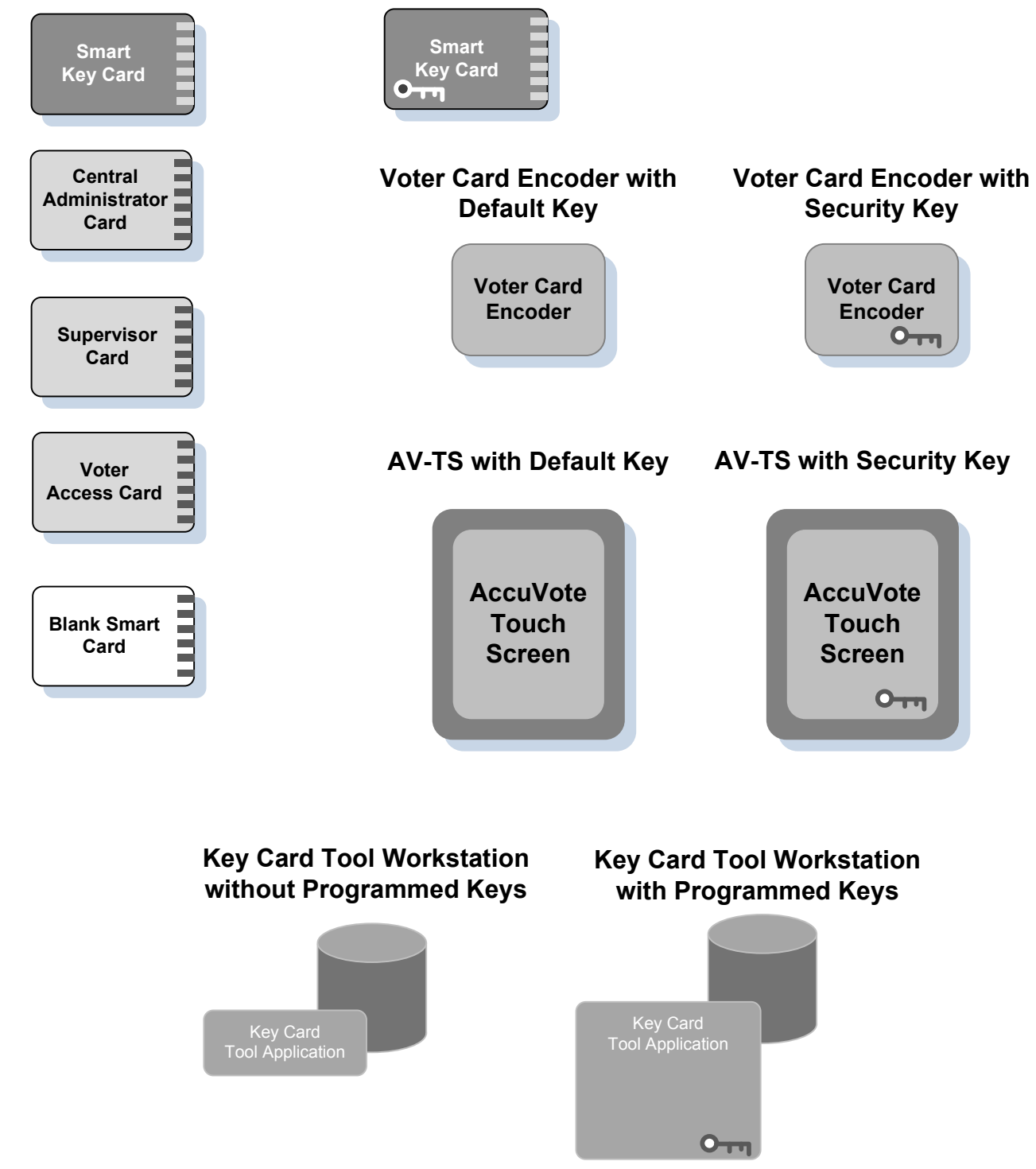


Premier Key Card Tool System Description			
Name:	Figure 4: Hardware Key Update		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	4 of 6





Premier Key Card Tool System Description			
Name:	Figure 5: Voting Process using Key Card		
Drawn By:	Mark Ayers	Date:	4/15/2008
Edited By:		Edited:	
Scale:	NTS	Sheet:	5 of 6



Premier Key Card Tool System Description			
Name:	Figure 6: System Overview Icon Legend		
Drawn By:	Mark Ayers	Date:	*4/15/2008*
Edited By:		Edited:	
Scale:	*NTS*	Sheet:	*6 of 6*

Appendix Q – Summary of Absentee Voting

Absentee Voting is a major component of the election process because, in the last election, 18% of the voters voted by absentee.

There are two broad categories of absentee voting. The first category includes **absentee** by (1.) mail, (2.) fax and (3.) special advanced requests. The second category is called **in person absentee** which includes (1.) special needs voting, (2.) early voting, and (3.) absentee in person.

The description of requirements is listed in the Division of Election web site. In all cases, the process starts with the request for ballots to be printed. This is done as part of the same order for ballots to the printer for the precinct voting 48 days before the election. The ballots are numbered in sequence with numbers of ballots printed from estimates based on previous elections.

Law requires that all absentee ballots be reviewed, opened and counted by the 15th day after the election. Absentee ballots are not part of the post-election audit process.

There is an **Absentee Voting Station Official Procedures** (Rev 5/2006) and a **Absentee Voting Official's Handbook** (Rev 4/25/06)

1. Absentee Ballots

Category 1 ballots are sent to the Division of Elections Absentee and Petition office in Anchorage by the printer.

1.1 Absentee by Mail

Deadline for by mail requests must be received 10 days before the election. Individuals can request either to vote for a single election or all elections in the calendar year. Voters receive their ballot by mail, complete it, and place the completed ballot into an included security sleeve. That is place that inside a return envelope, the envelope is signed and witnessed. The ballot envelope must be postmarked no later than Election Day. If mailed from within the United States, the envelope must be received within 10 days after Election Day. If mailed from outside the United States, it must be received within 15 days of Election Day.

The **by mail absentee** ballots are addressed to the respective Regional office. These envelopes are reviewed by the review board, opened and processed through an OS machines at the Regional office election evening. Either a separate machine is used or a OS machines that was used at the election, but with a separate memory card. Eligibility of absentee voters is accomplished with the Voter Registration Election Management System (VREMS). This system is completely separate from the GEMS system.

1.2 Absentee by Fax

GEMS generates the ballots **by fax** document as a PDF template that is distributed (faxed by computer) to those who requested the ballot by fax. Voters requesting this format can do so between 15 days before the election but no later that 5PM AST the day before Election Day. Voters have two options when receiving the ballot by fax. One is to return it **by fax** (to the Absentee and Petition Office) and the other is to **mail** it back to the respective Region Office. If faxed back, it must be received no later than 8 PM AST the day of the election. If mailed back, the ballot must be postmarked no later than the Election Day and received; within 10 days, if U.S postmarked or within 15 days if via international mail. Absentee voters are reminded that by returning their ballot by fax, means that they are voluntarily waiving their right to a secret ballot. Faxed ballots are sent from the Absentee and Petition office to the

respective Regional Office. The Region review board reviews each ballot for eligibility and determined if a full or partial count ballot. Ballots are placed in piles and two individuals together make a facsimile of the ballot for processing as an OS ballot.

1.3 Special Advance

This form of voting is available for individuals in remote Alaska or overseas who want an official ballot 60 – 32 days before the election. These requests result in the individual being sent both a special advance ballot and an official ballot to be voted absentee. If only the advanced ballot is returned to the Absentee office, it is entered into VREMS, and secured until 15 days after the election. The special advanced ballots are hand counted and the results manually loaded into GEMS. If the OS ballot is returned, it is entered into VREMS and forwarded to the respective Regional official. VREMS verifies if only the advanced ballot was received or if both the advanced ballot and the OS ballot were received. If both were received, the OS ballot is the only one that is counted. The Advanced ballots are accumulated to 15 days, then logged, reviewed by a review board and shipped to Juneau and entered officially in Juneau into GEMS.

2. In Person Absentee Voting

2.1 In person

Individuals may vote in person or through a representative up to 15 days prior to Election Day. Ballots are printed and delivered to the Regional offices. Each region has appointed absentee voting locations and distributes ballots to these locations. Some have house seat ballots for all 40 house seats and other absentee sites have only the ballots for the respective Regions' House Districts for that voting location. The Regional Offices (and Wasilla satellite are also absentee voting locations with ballots of all 40 representative districts and available for all 15 days.

Region	Number of Locations
I	30
II	11
III	20
IV	15

Some of the absentee voting locations are only available for Election Day or Election Day and the day before. The Official Election Pamphlets outline the locations and time that these locations are open for absentee voting.

2.2 Special Needs Voting

A qualified voter who is disabled may apply for an absentee ballot through a personal representative who can bring the ballot to the voter.
(following bullets taken from Division of Elections web site:
http://www.elections.alaska.gov/abinfo.php)

- A personal representative can be anyone over 18, except a candidate for office in the election, the voter's employer, an agent of the voter's employer, or an officer or agent of the voter's union.
- Ballots are available 15 days before the Primary, General or Statewide Special Election at any Regional Elections Office:

  - **Anchorage:** 2525 Gambell St, Ste 100 , 522-8683
  - **Fairbanks:** State Office Building, 675 7th Ave., 451-2835

- **Juneau:** Mendenhall Mall, 9109 Mendenhall Mall Road, Suite 3, 465-3021
- **Nome :** 103 E Front Street, 2nd Floor - State Office Building, 443-5285
- **Matanuska-Susitna :** 1700 E. Bogard Road, Building B, Suite 102 - North fork Professional Building, 373-8952

- Ballots are available 15 days before the Primary, General or Statewide Special Election from any Absentee Voting Official.
- Ballots are also available on Election Day from the voter's polling place, unless there is an Absentee Official in the area.
- The Personal Representative brings the completed application to an Election Official for a ballot and takes the ballot to the voter.
- The voter completes a certificate authorizing the Personal Representative to carry their ballot, votes the ballot privately, places it in a secrecy sleeve and seals it inside the envelope provided.
- The Personal Representative brings the voted ballot back to the Election Official by 8:00 p.m. on Election Day.

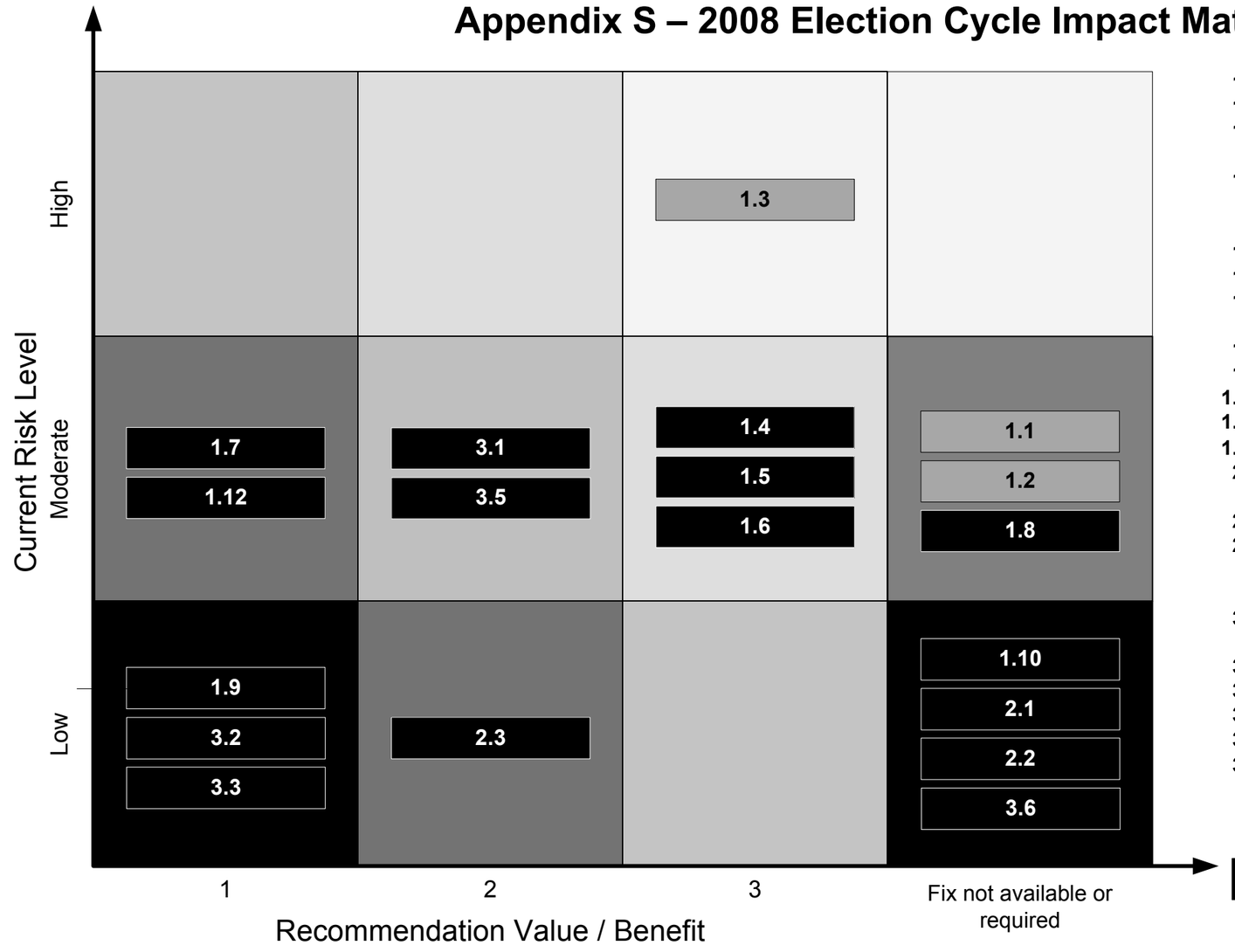
2.3 Early Voting In Person

These **early vote in person** ballots are only issued at the Regional offices (and Wasilla office). They are voted in the office and then sealed, placed in a separate ballot box. These ballots are opened and OS scanned election night with the ballots retuned to Juneau with the Regions election documents.

Appendix R – Master Matrix: Recommendations, Risk and Value Assessment

Document Section	Scope of Work Item	Current Risk Level (H, M, L)	Current Election Cycle Recommendation	Value / Benefit of implementing recommendation in the 2008 election cycle (3, 2, 1)	Residual Risk Level after implementation of 2008 election cycle recommendations (H, M, L)	Future Election Cycle Recommendation	Residual Risk remaining from 2008 election cycle (H, M, L)	Value / Benefit of implementing recommendation in the current election cycle (3, 2, 1)	Residual Risk Level after implementation of future election cycle recommendations (H, M, L)	Constraints / Notes
1.0	**Defense in Depth**									
1.1	Assure 1.2 Upgrade Cost Analysis	M	Maintain current revision of AccuVote software, perform cost benefit analysis to determine best resource utilization approach.	N/A	M	Upgrade to Assure 1.2 when certified	M	3	L	Funding and logistical planning of the upgrade represents a significant dedication of resources.
1.2	Assure 1.2 Functionality Upgrade Analysis	M	Maintain current revision of AccuVote software.	N/A	M	Upgrade to Assure 1.2 when certified	M	3	L	Certification of the Assure 1.2 software is required prior to installation.
1.3	Division of Elections Security Enhancements and Features Analysis	H	Implement selected recommendations from Appendix D - Division of Elections Enhancement Analysis. 2.1-2.5, 2.8, 2.10, 2.13, 2.16, 2.17, 2.18, 2.19, 2.23, 2.29	3	M	Implement remaining recommendations included in Appendix D.	M	3	L	Determination of which selected enhancements are implemented in the current election cycle requires input from the Division of Elections.
1.4	Implement procedures to minimize technology risks not addressed by existing or upgraded systems	M	Implement procedures described in other sections. Important to maintain many of the processes already in place.	3	L	Monitor research on election processes and implement changes, as appropriate.	L	2	L	Implementation of technology updates and changes is crucial to maintaining election system security and performance.
1.5	Password Management	M	Change passwords on all affected hardware as outlined in password management plan (Appendix E).	3	L	Develop password management procedures to implement password changes and tracking for future election cycles to ensure password policies are followed consistently.	L	2	L	Resources to develop password management procedures will likely not be available until after the 2008 election cycle.
1.6	Chain of Custody	M	Use tamper evident seals on AV-OS and AV-TSX machines.	3	L	Implement EPROM bar code identification and inventory management.	L	2	L	Bypass mail, rural home storage, poll worker training and uncertainty about tampering false alarms present challenges to implementing a robust tamper seal security plan.
1.7	Best practices for equipment storage between elections	M	Follow Chain of Custody recommendations. Purchase Division of Elections owned equipment for North Slope Borough. Safes are recommended for use in DoE offices to store keys and passwords.	1	L	Improve physical storage security such as room security, access alarm, etc.	L	3	L	Equipment storage outside of regional centers and hubs is not addressed by the recommendation. Security during transportation is a concern.
1.8	Trusted Personnel and single points of access	M	None	N/A	M	Require background checks on new employees with access to election equipment and confidential information	M	2	L	State and union regulations may limit the implementation of background checks. Access to proprietary information should be limited.
1.9	Redundancy	L	Two person inspection and sign off on tamper evident seals.	1	L	Add two-person sign-off to manual entry of election results and tamper seal inspections.	L	2	L	Poll worker resource constraints could make tamper seal inspections difficult on election day.
1.10	Paper Ballot tampering vulnerability	L	None	N/A	L	None	L	N/A	L	Maintain current paper ballot system.
1.11	Master Vulnerability Matrix	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
1.12	Security Training	M	Develop materials to train poll worker in election security.	1	L	Monitor new procedures and implement as appropriate.	L	1	L	Poll workers are temporary employees, usually retirees, many don't complete training, a lot of information to cover in training session, limits to poll worker authority.
2.0	**Fortification of Systems**									
2.1	Assess the integrity of the hardware and software of the electronic voting systems and their ability to accurately tabulate and report results.	L	Implement Key Card Tool application. Implement GEMS Air Gap Server model system. Implement dedicated AV-OS machine for programming AV-OS memory cards.	N/A	L	None	L	N/A	L	None
2.2	Preliminary Results Data Collection Assessment	L	None	N/A	L	None	L	N/A	L	None
2.3	Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.	L	Implement new shipping containers for optical scanning systems (Pelican™. Products 1600 series or similar)	2	L	None	L	1	L	None
3.0	**Confidence in Outcomes**									
3.1	Procedures for functionality, logic and accuracy testing for systems and memory cards.	M	Implement increased test scope for functional, logic and accuracy testing.	2	L	Implement test results documentation and storage policies.	L	2	L	Storage of machine test results may require implementation of an electronic data storage system.
3.2	Methods to improve voter confidence	L	Increase voter use of AV-TSX machines to improve voter anonymity.	1	L	Monitor research on election processes and implement changes, as appropriate.	L	N/A	L	Changes to Alaska's audit procedure require legislative approval. DoE staff size limits is ability to develop new poll worker training and recruitment programs.
3.3	Metrics and continuous improvement	L	Implement a multi-year, multi-phase approach to improving election procedures and equipment.	1	L	Multi-year, multi-phase approach	L	2	L	A multi-year, multi-phase approach requires staff training and coordination between DOE departments.
3.4	Weekly email summary	N/A	Provide on-going summary	N/A	N/A	Provide on-going summary	N/A	N/A	N/A	
3.5	Absentee and questioned ballot process	M	Implement 2008 election cycle security improvements.	2	L	Same as current election recommendations.	L	2	L	The absentee ballot system is subject to the same vulnerabilities as the standard election system but the AV-OS machines are exposed for a 2 week period of time.
3.6	Random sampling methodologies	L	None. Current research is not conclusive enough to recommend a change to the DoE methodology.	N/A	L	Implement new sampling procedure as appropriate and approved by statute.	Unknown	Unknown	Unknown	Changes must be approved by statute

Appendix S – 2008 Election Cycle Impact Matrix

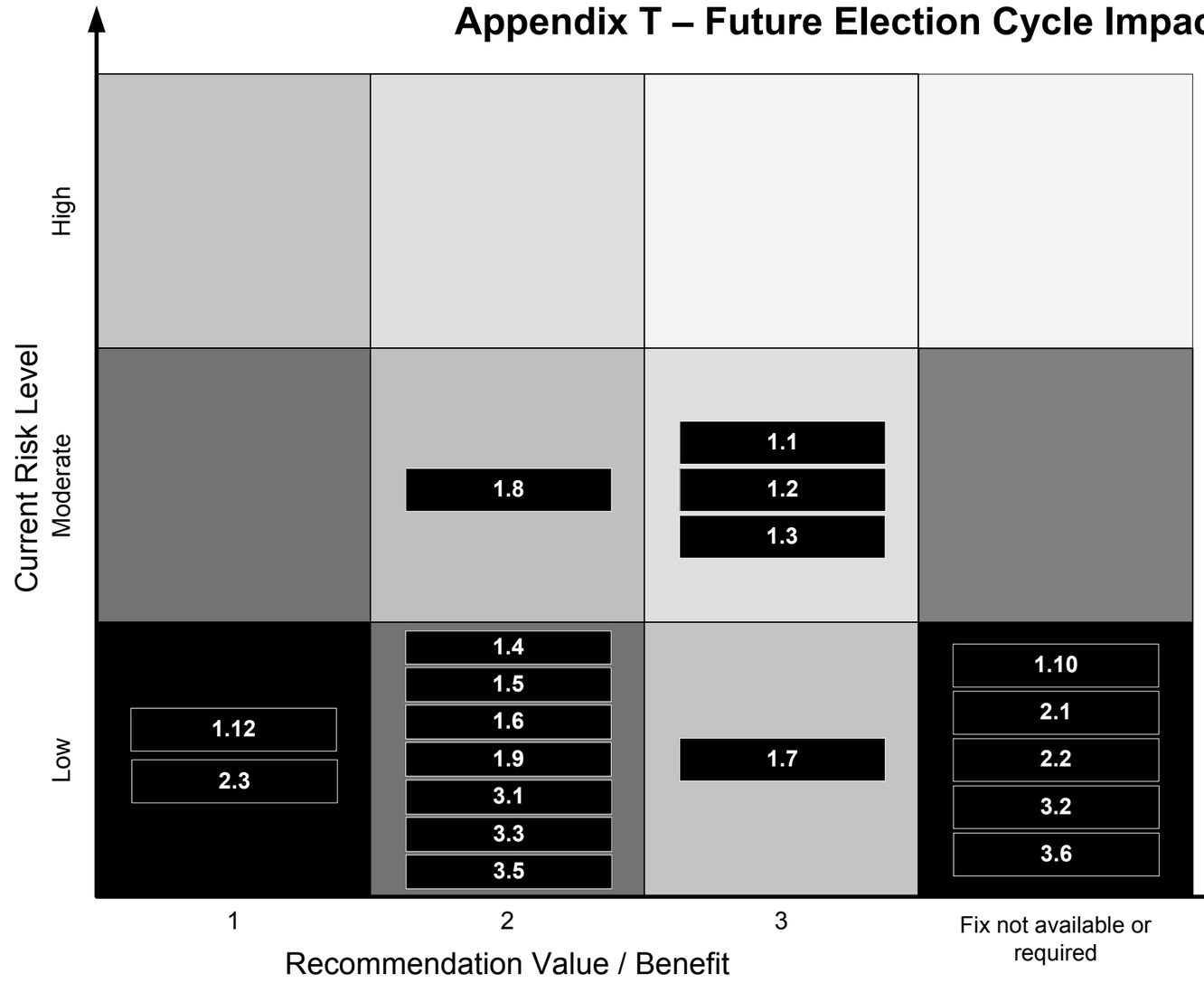


1.1 Assure 1.2 Upgrade Cost Analysis
1.2 Assure 1.2 Functionality Upgrade Analysis
1.3 Division of Elections Security Enhancements and Features Analysis
1.4 Implement procedures to minimize technology risks not addressed by existing or upgraded systems
1.5 Password Management
1.6 Chain of Custody
1.7 Best practices for equipment storage between elections
1.8 Trusted Personnel and single points of access
1.9 Redundancy
1.10 Paper Ballot tampering vulnerability
1.11 Master Vulnerabilty Matrix
1.12 Security Training
2.1 Communications Protocols, Integrity of hardware and software, perceived usability issues.
2.2 Preliminary Results Data Collection Assessment
2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.
3.1 Procedures for functionaity, logic and accuracy testing for systems and memory cards.
3.2 Methods to improve voter confidence
3.3 Metrics and continuous improvement
3.4 Weekly email summary
3.5 Absentee and questioned ballot process
3.6 Random sampling methodologies

Residual Risk Level

Low | **Moderate** | **High**

Appendix T – Future Election Cycle Impact Matrix



1.1 Assure 1.2 Upgrade Cost Analysis
1.2 Assure 1.2 Functionality Upgrade Analysis
1.3 Division of Elections Security Enhancements and Features Analysis
1.4 Implement procedures to minimize technology risks not addressed by existing or upgraded systems
1.5 Password Management
1.6 Chain of Custody
1.7 Best practices for equipment storage between elections
1.8 Trusted Personnel and single points of access
1.9 Redundancy
1.10 Paper Ballot tampering vulnerability
1.11 Master Vulnerabilty Matrix
1.12 Security Training
2.1 Communications Protocols, Integrity of hardware and software, perceived usability issues.
2.2 Preliminary Results Data Collection Assessment
2.3 Evaluate the reliability and accuracy of the optical scanning and touch screen systems in Alaska weather and transportation/handling conditions.
3.1 Procedures for functionaity, logic and accuracy testing for systems and memory cards.
3.2 Methods to improve voter confidence
3.3 Metrics and continuous improvement
3.4 Weekly email summary
3.5 Absentee and questioned ballot process
3.6 Random sampling methodologies

Residual Risk Level

Low | **Moderate** | **High**

Appendix U: Photographs of System Components and Division of Elections Facilities

1.0 Alaska Division of Election Voting Equipment

AccuVote-OS (Optical Scan Terminal)

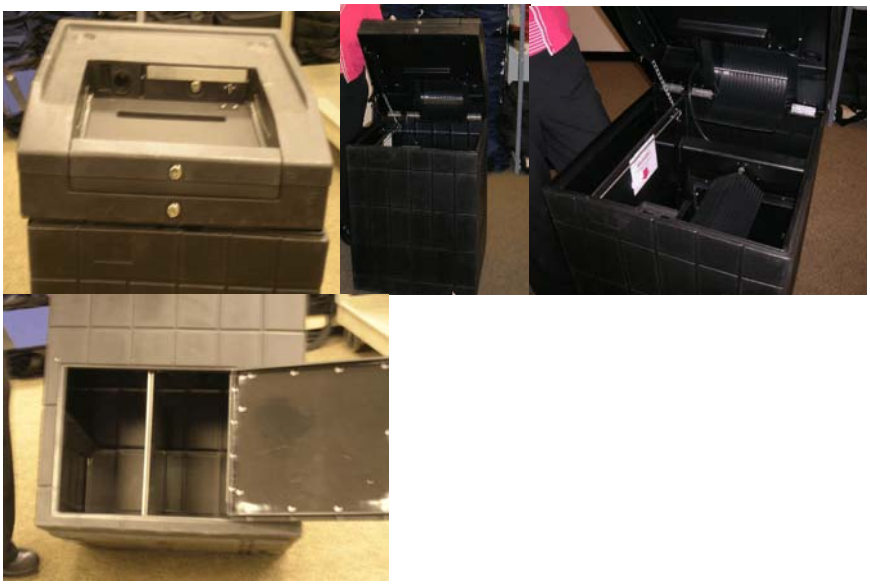
AccuVote-OS memory card port, memory card and panel to secure memory card in terminal.

Accuvote-OS Memory Card port secured with tamper evident, numbered tab. Tamper evident tab after removal.

AccuVote-OS Terminal vote recording tape chamber and tape. Tape is Secured beneath locked panel during election.

AccuVote-OS Terminal positioned over ballot container. Note lockable panel on ballot box is opened (lower left) . During election, locked front and rear panels of the ballot box coverthe secured memory card port and the rear of AccuVote OS unit (lower right).

Dual chamber, secure ballot container



Global Election Management System (GEMS) Server

GEMS Server (Fairbanks and Anchorage)

AccuVote-TXS (Touch Screen Voting Terminal)

AccuVote-TXS voting terminal, vote viewing panel and vote recording paper tape reel beneath lockable panel.

AccuVote-TXS voting terminal lockable memory card port and voter access card port.

2. Alaska Division of Elections Statewide, Regional and Borough Office's Equipment Storage

2.1 Juneau State-wide Office

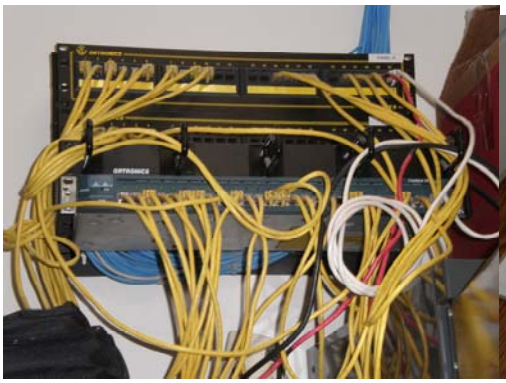
Election Programming Office keyed alarm panel and dead-bolt lock on door.

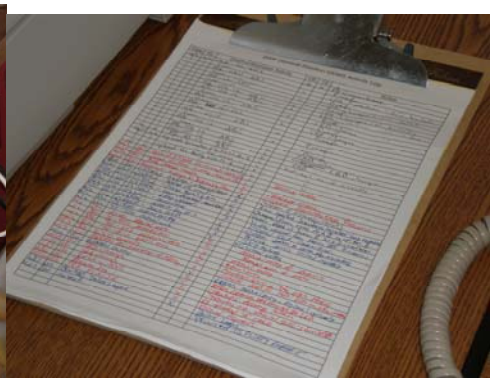
Election Programming Office Memory Card Storage Cabinet Memory Card Storage

Inside election programming office, GEMS Server and AV OS used for Memory Card programming prior to elections.

Inside AV-OS Unit: EPROM. Create barcode an place on underside of EPROM for security and inventory control

Switching Equipment in Election Programming Office and Equipment Action Log





Ballot Room

2.2 Region 1: Juneau

Alarm panel and memory card storage cabinet

GEMS Server

Walls and Ceiling

AV-OS Unit Storage

Inventory tags on shelves matched with individual AV-OS units.

AV-TSX Storage

2.3 Region 2: Anchorage

AccuVote-OS and AccuVote-TSX Storage areas.

AccuVote-TSX Voter Access Card programming units used at precincts. Numeric touch-pad alarm unit inside equipment storage room

2.4 Region 3: Fairbanks

(At the time of this photo the optical scanning equipment was on loan to the Fairbanks North Star Borough for their municipal election.)

2.5 Kenai Borough Office (Representative Hub)

Storage Vault

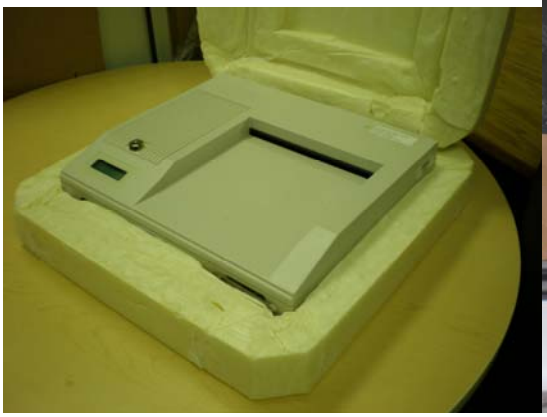
Equipment Storage inside Vault

Excess Election Material Storage

(Note: This material does not require secure storage (e.g. ballot boxes, tables, mailing envelopes, etc). No "secure" material is stored here (electronic equipment, ballots, etc.)

3.0 AV TSX and AV OS Shipping and Transportation

AV-OS foam padding and shipping boxes



AV-TSX Shipping Containers with locking capabilities

The AV-TSX shipping container plus the AV-TSX unit together weigh in excess of 50 pounds. The exterior latches on the AV-TSX shipping cases can be secured with serial-numbered tamper evident seals similar to the ones shown below.

AV-TSX Shipping Labels: US Mail Priority, Return Receipt

State of Alaska
Election Security Project:
Election Process Review
Phase 3 Report

Appendix D: Division of Elections: Election Process Review Statement of Work

FINAL
Division of Election
Election Process Review
5/17/2011

Goal:

Conduct a review of tabulation equipment, ballot security (pre, during and post-election), and audit post-election processes and procedures used by the Division of Elections in anticipation of the 2012 elections. Identify those areas where improvements could be made to ensure the division's tabulation equipment, voter history, ballot security and review, and election audit procedures are secure, effective and maintain the public's trust in Alaska's election system. In addition, review the division's processes to ensure non-US citizens and felons convicted of moral turpitude are not registered and/or voting.

Areas of Concentration:

1. Re-validate tabulation equipment security.
2. Review ballot security (pre, during and post-election).
3. Review post-election audit procedures and hand-count verification procedures.
4. Review systems that can improve real time access to and more efficient processing of voter history
5. Review methods used by division relating to felons and non-US citizens.

Proposed Method for Study:

The Division of Elections partners with the University of Alaska, Anchorage (UAA) to review the specified areas of concentration. Based on the outcomes of the studies, UAA makes recommendations on improvements within the environmental and statutory constraints that the Division of Elections works in.

Proposed Scope of Work:

Tabulation Equipment Security-Revalidate tabulation equipment security building on foundation of original study completed in 2008.

Ballot Security - The processes used to secure ballots (pre, during and post- election) between various polling locations and the Division of Elections, as well as the security once received by the division, will be reviewed to ensure ballots are secure and accounted for before, during and after transport, and to identify any necessary improvements. In addition, the processes and procedures relating to accountability and destruction of unvoted ballots after an election will be reviewed to ensure unvoted ballots cannot be later added to the election results. The study will identify improvements needed to ensure ballot accountability.

Post-election Audit Procedures – The methods and audit procedures used by the division's absentee and questioned ballot review boards and the State Ballot Counting Review Board (SRB), including the hand-count verification, to certify the election results should be reviewed to determine if the audit processes currently used would identify potential discrepancies in reported results and to recommend changes that would improve audit procedures. In addition, a review of the post-election processes would increase the public's confidence in the election results and identify any information that might be necessary to answer questions in the event of an election challenge.

Voter History – When entering a polling place, voters sign a precinct register prior to being given a ballot. All registers are returned to the division following the election and each voter who signed the register is given voter history on their official voter registration record. This history is entered manually by division staff and must be completed before the division opens and counts absentee and questioned ballots. In addition, in order for political parties and/or candidates to determine which voters have voted in an election, they currently need to station poll watchers at precincts to record voter names or wait until the division has performed the voter history. A review of the procedures used by the division to provide for voter history, researching feasibility of implementing electronic poll books and systems that might provide "real-time" access to and more efficient processing of voter history will be done to determine possible alternatives, including a cost/benefit analysis, timelines for, and risk assessment of such alternatives aligned with the 2012 election.

Felons and non-US Citizens – The processes and procedures used by the division to ensure felons convicted of moral turpitude and non-US Citizens are not registered and/or voting should be reviewed to determine if the division has access to, and receives information from, the necessary resources and data to identify such voters.

Proposed Approach

1. Conduct a review and audit of the procedures, processes, and technologies of the five areas of concentration identified for study (Revalidate Tabulation Equipment Security, Review ballot security, Review post-election audit procedures and hand-count verification procedures, Review "real-time" systems that can improve access to and more efficient processing of voter history, and Review methods used by division relating to felons and non-US citizens)
2. Survey other US jurisdictions to identify alternative approaches and best practices compared to the system in Alaska (both urban and rural environments).
3. Identify any gaps or concerns for Alaska
4. Provide assessment of alternatives for implementation and risk assessment aligned with 2012 election.
5. Conduct "pilot" test (possibly live election environment-REAA or Coastal Resource Service Area Elections in October in select location(s)) using selected

processes, technologies, and approaches to get feedback and suggest alternatives, timelines, and assess risks associated with 2012 implementation.
6. Analyze and audit post-election procedures.
7. Produce final written report, presentation and other deliverables as defined.

Phase 0: (Mid April-End May)

1. Finalize scope of work, develop overall project plan, and clarify deliverables.
2. Establish team (UAA, ISER, DOE), contacts, key stakeholders, and communication plan.
3. Get contracts in place (Use RSA approach leveraged from previous studies).
4. Consolidate and transfer relevant background documentation from DOE.

Phase 1: ~ Beginning June-end September

1. Audit current procedures (SOW Items #1-5) and document.
2. Evaluate other US State jurisdictions and summarize how they approach similar issues and their application of different technologies/processes/approaches.
3. Identify best practices and determine gaps in Alaska system/approach.
4. Provide recommendations for specific approaches to close gaps/strengthen current approaches that might be incorporated into Oct REAA election or a mock-election (July-August).
5. Produce detailed and summary report and presentations (as requested).

Phase 2: ~ Beginning October- Beginning December

1. Assist with implementation of targeted changes (if requested).
2. Audit post-election processes of live REAA election in October 2011 in selected locations.
3. Test out selected process and technology recommendations (with consideration to scalability to larger elections) either during live REAA election in October or mock election.
4. Produce follow up report with observations and lessons learned from live election (or mock-up) audit.

<u>Team:</u>

- LuAnn Piccard, Interim Director, UAA Engineering, Science and Project Management (ESPM)
- Mark Ayers, UAA Faculty (School of Engineering)
- Dave Hoffman, UAA Faculty (ESPM)
- Roger Hull, UAA Faculty (ESPM)
- Michelle Whitney, UAA ESPM Project Coordinator
- Mary Killorin, ISER

- Stephanie Martin, ISER

Budget: Rough Budgetary Estimate +/- 50% (subject to further detailed discussions):

- $200K (Personnel, F&A, Travel, Misc.)